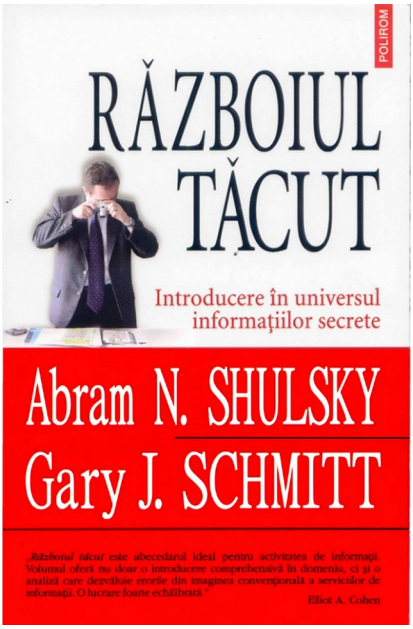
POLIROM
RĂZBOIUL TĂCUT
Introducere în universul informaţiilor secrete
Abram N. SHULSKY
Gary J. SCHMITT
„Războiul tăcut este abecedarul ideal pentru activitatea de informaţii. Volumul oferă nu doar o introducere cuprinzătoare în domeniu, ci şi o analiză care dezvăluie erorile din imaginea convenţională a serviciilor de informaţii. O lucrare foarte echilibrată."
Elliot A. Cohen

Abram N. Shulsky, Gary J. Schmitt, *Silent Warfare*. *Understanding the World of Intelligence*, 3* Edition

Copyright 2002 by Potomac Books, Inc.

Published in the United States by Potomac Books, Inc. All rights reserved. No part of this book may be reproduced în any manner whatsoever without written permission from the publisher, except in the case of brief quotations embodied în criticai articles and reviews.

First edition published 1991. Second edition published 1993. Third edition 2002.

Excerpt from *Strategic Intelligence for American World Policyby* Sherman Kent.

Copyright 1949 by Princeton University Press.

Copyright renewed 1976 by Princeton University Press.

Reprinted with permission of Princeton University Press.

Excerpts from *Secrecy and Democracy*: *The CIA* in *Transition* by Adm. Stansfield Turner.

Copyright 1985 by Stansfield Turner.

Reprinted by permission of Houghton Mifflin Company.

2008 by Editura POLIROM

www.polirom.ro
Editura POLIROM
laşi, B-dul Carol I nr. 4

Descrierea CIP a Bibliotecii Naţionale a României: SHULSKY, ABRAM N.

Războiul tăcut: introducere în universul informaţiilor secrete /

Abram N. Shulsky şi Gary J. Schmitt; trad. de Laura-Florina Drăghici, Cristina Dogaru, Maria-Adelina Negoiţă şi Irina-lonela Bondar; cuv. Înainte de George Maior; postf.: Mihai-Răzvan Ungureanu. – laşi: Polirom, 2008 Index

ISBN: 978 – 973 – 681 – 733 – 5

I. Schmitt, Gary, J.
II. Drăghici, Laura (trad.)
III. Dogaru, Cristina (trad.)
IV. Negoiţă, Maria-Adelina (trad.)
V. Bondar, Irina (trad.)
VI. Maior, George Cristian (pref.)
VII. Ungureanu, Mihai-Răzvan (postf.)

351.746.1 (498) 327.84 (498)

# RĂZBOIUL TĂCUT

Introducere în universul informaţiilor secrete

Abram N. SHULSKY
Gary J. SCHMITT

Traducere de Laura-Florina Drăghici, Cristina Dogaru, Maria-Adelina Negoiţă şi Irina-Ionela Bondar
Cuvânt înainte de George Maior
Postfaţă de Mihai-Răzvan Ungureanu
POLIROM 2008

Abrain N. Shulsky, când a scris *Războiul tăcut*, era un membru marcant al Naţional Strategy Information Center (NSIC) din Washington, DC. În prezent lucrează la Washington, unde este consultant pe probleme de securitate naţională. Anterior, a făcut parte din echipa de planificare a strategiilor politice din cadrul Cabinetului secretarului de stat american al Apărării. A fost coordonator al politicii privind controlul strategic al armelor din cadrul Pentagonului şi director al subcomisiei din cadrul Comisiei speciale pentru activitatea de informaţii a Senatului. De asemenea, a fost consultantul Consiliului de experţi pe probleme de informaţii externe al preşedintelui şi reprezentantul secretarului de stat american al Apărării la negocierile pe probleme nucleare şi privind spaţiul cosmic de la Geneva dintre SUA ŞI URSS. Este autorul mai multor articole referitoare la serviciile de informaţii şi problematica securităţii naţionale.

Gary J. Schmitt este preşedinte al Proiectului pentru un nou Secol American (Project for the New American Century), un grup de experţi specializat pe probleme de securitate naţională. A fost director-executiv al Consiliului de experţi pe probleme de informaţii externe al preşedintelui SUA şi director al subcomisiei din cadrul Comisiei speciale pentru activitatea de informaţii a Senatului. De asemenea, a fost consultant pentru Departamentul Apărării din SUA. Este autorul mai multor lucrări privind probleme de securitate naţională şi guvernul american.

**Cuprins**

*Cuvânt înainte* (George Maior) …
*Prefaţă*…
*Către cititor*…
Introducere. A scrie despre secrete…
Capitolul 1. Ce este activitatea de informaţii? …
Delimitarea domeniului…
Serviciile secrete şi era informaţională…
Elementele activităţii serviciilor de informaţii…
Capitolul 2. Spioni, maşini şi biblioteci: culegerea informaţiilor
Culegerea informaţiilor din surse umane…
Culegerea informaţiilor din surse tehnice…
Comparaţie între *humint* şi *techint*…
Culegerea informaţiilor din surse deschise…
Capitolul 3. Ce înseamnă toate acestea?
Analiza şi producerea informaţiilor…
Ce este analiza?…
Produsul activităţii serviciilor de informaţii…
Eşecurile serviciilor de informaţii şi evenimentele neprevăzute…
Capitolul 4. În culise: operaţiunile secrete: …
Ce sunt operaţiunile secrete?…
Tipuri şi exemple de acţiuni secrete…?…
Acţiunile secrete şi păstrarea confidenţialităţii…
Acţiunile secrete şi activitatea de informaţii…
Capitolul 5. Spion contra spion: activitatea de contrainformaţii…
Clasificarea informaţiilor…

Securitatea…
Contraspionajul…
Activităţi contrainformative multidisciplinare (MDCI) …
Dezinformare şi contradezinformare…
Analiza contrainformativă…
Capitolul 6. Controlul paznicilor: managementul culegerii informaţiilor…
Caracterul secret şi controlul…
Expertiză şi strategie…
Serviciile secrete şi „era informaţională”…
Activitatea de informaţii şi democraţia…
Capitolul 7. Două perspective asupra lumii informaţiilor…
Istoricul viziunii americane…
Activitatea de informaţii şi problemele etice…
Capitolul 8. Elemente pentru o teorie a culegerii informaţiilor
*Note*…
*Postfaţă* (Mihai-Răzvan Ungureanu) …
*Index*…

Cuvânt înainte

Deşi în era globalizării şi în contextul de după 11 septembrie 2001 activitatea serviciilor de informaţii din întregul spaţiu euroatlantic a devenit unul din subiectele importante ale mass-mediei internaţionale, universul informaţiilor secrete rămâne puţin cunoscut publicului din România. În SUA şi în Marea Britanie, precum şi în alte state occidentale, domeniul *intelligence* şi al reformei serviciilor de informaţii a făcut în ultimii ani obiectul unor intense dezbateri academice în conexiune directă cu modificările

majore ale conceptelor de *securitate naţională*, *apărare*, *război* şi *pace* în secolul XXI. În România însă, dezbaterile publice au fost adesea canalizate, din raţiuni evidente şi explicabile, spre analiza trecutului, spre desprinderea de moştenirea istorică a fostei Securităţi şi mai puţin spre viitorul *intelligence* şi pe rolul acestui domeniu extrem de sensibil în planul mai larg al securităţii şi cooperării internaţionale.

Din această perspectivă, consider că publicarea volumului *Războiul tăcut* (*Silent Warfare*) acoperă un deficit real de informaţie asupra a ceea ce înseamnă munca de *intelligence*, spionajul şi contraspionajul, analiza de informaţii, acţiunile şi operaţiunile concrete din acest domeniu. Autorii, Abram N. Shulsky şi Gary J. Schmitt, îşi propun în a treia ediţie a cărţii să dezvolte un adevărat manual al muncii de informaţii, prin care, în plan didactic, să clarifice concepte-cheie în domeniul operaţional, precum sursele, agenţii, activităţile sub acoperire, manipularea adversarului, modalităţile de culegere a informaţiilor din surse tehnice şi varietatea acestora. Pornind de la aceste date de bază, cartea merge însă mult mai departe, în substanţa relaţiilor dintre serviciile de informaţii şi factorii de decizie în stat, analiza impactului *intelligence* asupra politicilor naţionale, aspectele morale şi de control civil şi democratic, echilibrul şi tensiunile inerente între eficienţă şi legitimitate publică, între lupta secretă de zi cu zi care se duce în acest domeniu şi valoarea sa strategică în timp.

Dezvoltarea şi expansiunea dinamică a

tehnologiei, a mijloacelor de comunicaţie fac ca informaţia de orice tip să traverseze rapid graniţe şi hai icre administrative, comprimând geografia şi dând o semnificaţie diferită cunoaşterii într-un asemenea context. Cartea surprinde foarte bine tocmai consecinţele globalizării asupra *intelligence* – vulnerabilităţile, dar şi forţa unor sisteme naţionale fundamentale pentru asigurarea funcţiilor şi atribuţiilor vitale ale unui aparat statal în faţa expansiunii fără precedent a surselor de informaţii publice, în faţa unor tendinţe de apariţie a altor actori în domeniu (*intelligence* privat folosit în mediul de afaceri, dezvoltarea *think-tank-urilor* şi a organizaţiilor cu rol de analiză şi culegere a unor informaţii cu valoare strategică). Mă refer în mod explicit la vulnerabilităţi pentru că vedem astăzi cât de importantă şi dificilă este coroborarea informaţiilor provenite din diferite surse, umane şi tehnice, secrete şi deschise, atunci când volumul acestora a devenit imens, iar decelarea şi analiza importanţei lor pentru securitatea naţională tot mai problematice. Mă refer, de asemenea, la forţa serviciilor de informaţii în actualul mediu internaţional, pentru că bătăliile în prezent se poartă mai puţin pe câmpul de luptă clasic şi tot mai mult, în domeniul meta-politic al cunoaşterii şi înţelegerii unor fenomene.

Din această perspectivă, un serviciu de informaţii deţine o forţă deosebită în planul protejării şi promovării intereselor de securitate ale unui stat.

Spionajul şi contraspionajul, arta migăloasă şi

periculoasă a culegerii informaţiilor pentru stat, munca intelectuală în vederea analizării acestora, a interpretării lor sau cea de a-i transmite aceste informaţii decidentului politic, dincolo de constrângerile ideologice sau prejudecăţile birocratice, constituie şi astăzi diferite faţete ale aceleiaşi profesii vechi de când lumea. O profesie care se schimbă în mod fundamental în prezent – şi aici cartea lui Shulsky şi Schmitt vorbeşte de o adevărată Revoluţie în *Intelligence*, similară Revoluţiei în Afacerile Militare (RMA) dezvoltate în SUA în cadrul Pentagonului. Această revoluţie influenţează uneori în mod decisiv felul în care se desfăşoară anumite procese.

Structura cărţii are la bază principalele componente ale muncii de informaţii: culegerea, analiza, acţiunile sub acoperire şi contraspionajul (sau, cum spun autorii, lupta spionului cu spionul). În cazul fiecăruia dintre aceste aspecte sunt evaluate actualele tendinţe de evoluţie, eşecurile şi succesele în diferite momente din istoria modernă, modul în care se coagulează în final produsul de *intelligence* şi cum evoluează relaţiile dintre furnizorii de informaţii şi beneficiarii acestora.

Cartea încearcă să contrapună tendinţele şi orientările care au prevalat în istoria serviciilor americane de informaţii şi să extragă şi o serie de lecţii sau învăţăminte din acestea. Astfel, predilecţia pentru sursele tehnice şi extinderea exponenţială a domeniului, de la mijloacele clasice de interceptare la zona-satelit sau cercetarea radioelectronică, au condus la un moment dat la

diminuarea ponderii surselor umane, cu anumite consecinţe negative în planul culegerii şi valorificării informaţiilor. Totuşi, validarea surselor umane prin mijloace tehnice rămâne un subiect actual în comunitatea de informaţii a Statelor Unite. La nivelul contraspionajului, arta informaţiilor a ajuns la evoluţii surprinzătoare în manipularea adversarilor, infiltrarea agenţilor şi anticiparea deciziilor inamicului, în care putem compara activitatea de *intelligence* cu un adevărat joc de şah. Şi aici exemplele concrete, eşecurile fulminante sau succesele de multe ori tăcute au constituit o pagină fundamentală din istoria Războiului Rece. Operaţiunile sub acoperire constituie, de asemenea, o parte extrem de importantă a „jocului" cu adversarul – de la crizele politice determinate de scandalul Iran-Contra în SUA la sprijinul american pentru mujahedinii din Afganistan sau la acţiunile de propagandă şi influenţă, inclusiv ceea ce autorii numesc *blackpropaganda* (propagandă neatribuită) sau *grey propaganda* (cea realizată parţial deschis prin organizaţii precum Vocea Americii în perioada conflictului dintre cele două blocuri ideologice). Deşi relevanţa lor politică şi strategică a fost nu o dată contestată, este indiscutabil faptul că acestea rămân instrumente foarte importante ale serviciilor de informaţii. Autorii subliniază importanţa definirii acestor acţiuni în contextul unui control politic adecvat şi al asumării consecinţelor lor.

Trebuie înţeles însă faptul că *intelligence* este o luptă nu numai pentru prevenire şi protecţie, în

sens clasic, ci şi – sau mai ales – pentru promovarea unor interese ale statului, sesizarea şi evaluarea unor oportunităţi strategice de acţiune. În acest sens, este evident, aşa cum afirma Treverton, că, „în prezent, cel ce are o viziune adevărată nu este un spion de elită şi cu atât mai puţin un satelit impersonal, ci acea persoană pregătită să înţeleagă substanţa unor fenomene – un analist”[1].

Elementul fundamental pe care un analist de informaţii îl aduce în ecuaţia de securitate este cel al cunoaşterii strategice. Aceasta constituie un factor esenţial pentru luarea unor decizii corecte în aplicarea politicii externe a statelor, în promovarea intereselor acestora. Este însă foarte greu de definit. Totuşi, poate fi vorba de acel tip de cunoaştere esenţială care, pe de o parte, face la nivel de sinteză, suma datelor fundamentale – de tip economic, militar, geopolitic şi strategic – referitoare la un anumit context internaţional, iar pe de altă parte, integrează analitic informaţiile privind dinamica proceselor care se răsfrâng ori s-ar putea răsfrânge asupra acestui context, selectându-le, bineînţeles, pe cele care au capacitatea de a-i determina decisiv evoluţia.

Ignorarea datelor şi a analizei care produc sau au potenţialul de a produce cunoaştere strategică poate avea consecinţe nefaste şi chiar primejdioase asupra orientării externe a statelor.

---

1 Gregory F. Treverton, *Reshaping* Na*tional Intelligence for an Age of Information*, Cambridge University Press, Cambridge, 2003, p. 10.

Istoria oferă numeroase exemple de acest fel. Într-adevăr, aşa cum sublinia Charles Kupchan în monumentala sa lucrare *Vulnerabilitatea Imperiului* (*The Vulnerability of Empire*), „distorsiunea psihologică, greşelile de calcul sau credinţele strategice inadecvate, născute din constrângeri cognitive, pot determina elitele să urmeze strategii autodistructive…”. În orice caz, dacă elitele pot promova, din raţiuni subiective, interesate sau datorită altor tipuri de constrângeri (de exemplu, ideologice), „strategii autodistructive” sau falimentare din punctul de vedere al consecinţelor strategice sau geopolitice, este important ca ele să nu aibă niciodată scuza lipsei de cunoaştere strategică obiectivă în deciziile pe care le adoptă în momente cardinale ale istoriei. Adică a acelui flux informaţional fundamental, capabil să surprindă tabloul realităţii în liniile sale esenţiale, dar şi fotografia – cu cât mai puţine impurităţi – a viitorului. Cu alte cuvinte, ar fi extrem de grav dacă o linie politică sau strategică ar fi asumată în mod eronat, pe baza unor informaţii false, irelevante sau a unei analize greşite (tot istoria demonstrează că adesea decizia politică a fost greşită chiar dacă acel bagaj de informaţie strategică s-a aflat totuşi la îndemâna elitelor).

Cunoaşterea strategică nu trebuie confundată întotdeauna cu prognoza sau încercarea de estimare a viitorului, pe durate lungi de timp. Unii specialişti spun chiar că este o greşeală să defineşti cunoaşterea strategică prin prisma analizei pe termen lung, acest tip de cunoaştere

fiind cea care trebuie să iniţieze mai degrabă strategii şi politici strategice.

Totuşi, unul dintre cele mai ambiţioase produse intelectuale ale unei instituţii din domeniul *intelligence* este cel care încearcă să ofere prognoze sau predicţii asupra evoluţiei evenimentelor în sistemul relaţiilor internaţionale. A reuşi să oferi o perspectivă clară asupra a ceea ce s-ar putea întâmpla peste 5, 10 sau 15 ani în domeniul relaţiilor de putere (de exemplu, vom avea de-a face cu influenţa unei puteri care va continua să exercite supremaţia în raporturile internaţionale sau lumea va deveni mai multipolară?) are o semnificaţie aparte asupra orientării diplomaţiei şi politicii externe a statelor interesate; ea poate fundamenta o gândire strategică solidă.

Dar lista întrebărilor interesante şi importante din punct de vedere strategic este mult mai lungă şi se poate manifesta în diferite domenii de interes vital pentru state, de la cele de ordin geopolitic – „Va fi mai multă stabilitate în Orientul Mijlociu?”, „Se va integra Turcia în Uniunea Europeană?”, „Se va stabiliza Irakul?”, „Se vor reaprinde focare de instabilitate în Balcani prin declararea independenţei provinciei Kosovo? „– până la zone semnificative din sfera economică – „Va reuşi Uniunea Europeană să-şi diminueze dependenţa în ceea ce priveşte resursele energetice?”, „Se vor crea rute alternative de transport a hidrocarburilor din Asia Centrală către Europa? „Va creşte preţul petrolului? „etc.

Analiza de prognoză pe termen mediu şi lung

este întotdeauna un proiect extrem de ambiţios, dar şi unul foarte dificil şi riscant. În primul rând, testarea sa în raport cu evoluţiile efective din planul realităţii este cvasi-imposibil de realizat, dincolo de validitatea şi logica argumentaţiei şi construcţiei intelectuale desprinse ca atare din analiză şi din tipul de informaţie care stă la baza analizei. Bineînţeles, mai există şi testul inexorabil al timpului care poate valida sau nu o prognoză, însă acest lucru nu mai este important atunci decât din unghiul istoriei, în legitimarea retroactivă a credibilităţii analizei, a capacităţii sale originare de a anticipa într-adevăr evenimentele şi efectele lor.

În al doilea rând, serviciile de informaţii sunt în prezent axate pe validarea în plan tactic, operativ a acţiunilor şi informaţiilor obţinute, pe efectele imediate sau rapide ale unor decizii – oarecum similar, din acest punct de vedere, cu activitatea în politica externă şi în diplomaţie. Foarte rar instituţiile unui stat dispun de timpul şi resursele necesare pentru a se distanţa, din punct de vedere conceptual, de „agenda zilei” – cea care influenţează în mod curent deciziile politice în stat – pentru a putea să dezvolte şi să susţină prognoze pe termen lung.

Analiza predictivă sau strategică nu este, desigur, apanajul unei organizaţii de *informaţii*/*intelligence* sau a vreunei alte organizaţii guvernamentale. Mediile academice, mass-media, *think-tank-urile* se pot lansa şi se lansează în asemenea studii de prognoză, procesând şi interpretând informaţia valabilă

oricum din multitudinea de date disponibile la vedere, din surse deschise. Mai ales în era globalizării, creşterea dramatică a numărului canalelor de comunicare şi de transmitere a informaţiilor, diversificarea lor continuă fac posibile asemenea exerciţii intelectuale, iar „competiţia" cu sistemele oficiale devine una de tip metodologic, vizând posibile grile de interpretare, de alegere a unei anumite metode sau matrice de abordare pe care să se fundamenteze acest tip de cunoaştere cu valenţe prospective (poate însă să nu fie vorba neapărat de competiţie, ci de întrepătrunderi şi complementaritate între diverse perspective analitice şi interpretative). Cu alte cuvinte, e vorba de aceeaşi întreprindere intelectuală, cu prelungiri înspre rafinamentul şi profunzimea analizei, calitatea şi acurateţea sa intelectuală în modul de utilizare a metodelor deductive sau inductive, potenţialul de extrapolare a exemplelor istorice, în general a aplicării unor raţionamente specifice ştiinţelor sociale. Până la un punct, e vorba şi de un joc de imaginaţie şi de creativitate, dar acestea pot fi periculoase în lipsa cercetării riguroase, cantitative, şi calitative şi a aplicării unor metode ştiinţifice, critice.

Shulsky şi Schmitt încearcă să surprindă în concluziile cărţii tocmai această relaţie complexă dintre *intelligence* şi ştiinţele sociale, relaţie insuficient investigată, în opinia mea, până în prezent. Autorii propun o distincţie primară în care ştiinţele sociale anticipează şi analizează, în vreme ce *intelligence* este eficient în măsura în

care acţionează, adică – în baza analizei şi prognozei – construieşte şi fundamentează răspunsuri la actualele riscuri de securitate, manipulează adversarii şi schimbă uneori cursul strategic al istoriei (ceea ce ştiinţele sociale nu îşi pot propune).

Citat şi în acest volum, Sherman Kent, într-una dintre cele mai importante cărţi despre analiza strategică desfăşurată în serviciile de informaţii – *Strategic Intelligence for American World Policy* –, scria despre analogia dintre ştiinţele sociale şi produsul anticipativ care ar trebui să reprezinte unul dintre demersurile fundamentale ale *intelligence-ului*: „Cercetarea este singurul proces care noi, cei din tradiţia liberală suntem dispuşi să admitem că e capabil să ne ofere adevărul sau o aproximare a adevărului… Insistăm şi am insistat de generaţii că adevărul trebuie abordat, dacă nu şi obţinut, prin cercetare îndrumată de o metodă sistematică. În ştiinţele sociale, care în mare parte constituie materia informaţiei *intelligence* strategic, există o asemenea metodă. Este asemănătoare cu metoda din ştiinţele exacte. Nu e aceeaşi metodă, dar este o metodă fără îndoială". Iar William Colby, fost director al CIA, afirma în acelaşi spirit: „O nouă disciplină concepută special pentru analiza din *intelligence* trebuie rafinată, iar procesul de cercetare şi dezvoltare a început deja. Va merge dincolo de analiza academică prin noi tehnici capabile să proiecteze viitorul mai degrabă decât să explice trecutul. Experimentele în această nouă disciplină nu sunt nici pe departe limitate la

comunitatea oficială de informaţii întrucât ele se desfăşoară în centre de cercetare ştiinţifică, între analişti politici, în proiecţiile clubului de la Roma în alte locuri…”

Pare destul de deprimantă ideea că nu există anumite certitudini în ceea ce priveşte existenţa măcar a unui loc care să poată oferi predicţii categorice despre viitor. Nu este totuşi aşa.

Analiza strategică este relevantă pentru trasarea unui curs raţional al politicilor prin labirintul contextelor şi situaţiilor care structurează realitatea în dinamica sa. Analiza strategică poate elimina subiectivismul generat de percepţii sau interese imediate, de ideologii neclare, aducând lumină în zone altfel acoperite de vălul incertitudinilor şi al prejudecăţilor, de „ceaţa” faptelor neconcludente, parafrazându-l pe Clausewitz, sau a evenimentelor minore în raport cu marile mize politice. În fine, analiza strategică – stând practic la baza a ceea ce am putea numi cunoaştere strategică – este fundamentală în luarea deciziilor importante de către oamenii de stat, care altfel ar putea foarte bine să se ghideze precum ghicitorii după ceea ce pretind că (preţ văd în misterioasele lor „globuri de cristal”, aşa cum menţiona ironic un teoretician cunoscut al domeniului. De altfel, în legătură cu această ultimă problemă, Sherman Kent a lansat cu mult timp în urmă un serios avertisment intelectual: „Când concluziile analizei de *intelligence* sunt ignorate de consumator pe motivul intuiţiei acestuia, ar trebui să recunoască faptul că întoarce spatele celor două instrumente pe care

omul occidental le-a folosit, încă de la Aristotel, pentru lărgirea orizontului său de cunoaştere – instrumentul raţiunii şi cel al metodei ştiinţifice”.

Aici intervine şi un alt capitol al cărţii, de asemenea novator prin analiza propusă în planul cercetării din ţara noastră, ce reflectă relaţia complicată dintre *intelligence* şi politică. După cum spunea acelaşi Sherman Kent, „avertizarea strategică este precum dragostea, e nevoie de doi pentru aceasta” – uneori munca de *intelligence* nu reuşeşte să ofere soluţii factorilor de decizie, alteori aceştia din urmă ignoră importanţa informaţiilor şi preferă să acţioneze în mod subiectiv în stabilirea unor cursuri de acţiune, în fine uneori informaţiile nu sunt adecvate momentului strategic şi capătă valoare politică mai târziu, când sunt „uitate” într-un sertar.

Relaţia dintre informaţie şi decizie este fundamentală pentru eficienţa acţiunilor unui stat. Această relaţie trebuie gândită din perspectivă strategică, dar şi managerială – decuplând munca de informaţii de influenţele şi presiunile politice de moment, dar conectând-o la agenda politică şi la interesele perene ale securităţii naţionale.

Conectat acestor perspective, *Războiul tăcut* se termină cu o încercare de sinteză teoretică a fenomenului *intelligence* în care contrapune două mari direcţii de înţelegere a acestui domeniu – cea deschisă cu milenii în urmă de Sun Tzu privind cunoaşterea pură şi cea legată de relativismul posibilităţilor actuale de a opera cu concepte absolute în acest domeniu supus atâtor tipuri de constrângeri, inclusiv de tip cognitiv.

Perspectiva lui Shulsky este una esenţial critică, deşi acest tip de abordare riguroasă şi metodică pare să dăuneze preconcepţiilor romantice vizavi de acţiunile spionajului sau misterului care învăluie modul aparte de operare în această activitate sensibilă. Însă tocmai „demitizarea” operată de o lucrare ştiinţifică de un asemenea calibru are o semnificaţie deosebită pentru societatea civilă şi mediul academic din România: oferă o perspectivă ştiinţifică într-un domeniu supus mult prea multor mistificări şi politizări în trecut şi stabileşte un cadru de analiză obiectivă a viitorului muncii de informaţii într-o lume supusă schimbărilor permanente în care riscurile au devenit tot mai evazive, securitatea tot mai complexă, iar războaiele tot mai mult determinate de cunoaşterea şi utilizarea informaţiilor.

*George Maior*

## Prefaţă

*Războiul tăcut* îşi are originea într-un curs despre culegerea informaţiilor pe care l-am predat în 1985, când eram profesor asociat la John M. Olin Center for Inquiry into the Theory and Practice of Democracy, Universitatea din Chicago. Întoarcerea în lumea academică mi-a impus o organizare mai clară a ideilor mele privind lumea informaţiilor, subiect pe care-l cunoşteam datorită carierei mele de la Washington. Cartea a fost publicată pentru prima dată în 1991. La scurt timp, promovarea unor noi legi privind activitatea de informaţii, atât în SUA, cât şi în alte ţări, publicarea mai multor lucrări pe aceeaşi temă şi destrămarea Uniunii Sovietice au determinat publicarea unei ediţii revizuite a *Războiului tăcut*. Dar la momentul respectiv îmi reluasem deja funcţia de oficial guvernamental la Departamentul Apărării şi nu aveam suficient timp pentru a face adăugirile necesare. De aceea, l-am rugat pe Gary Schmitt, cel care m-a înlocuit în postul de director de personal la Comisia Parlamentară de Control al Serviciilor de Informaţii şi fost director executiv al Comitetului de Consultanţă al Preşedintelui privind Informaţiile Externe, să se ocupe de revizuirea cărţii. A doua ediţie a apărut în 1993.

În această perioadă, bibliografia şi resursele dedicate subiectului s-au diversificat. În plus, a crescut numărul legilor speciale de reglementare a domeniului informaţiilor în vederea armonizării reglementărilor deja existente cu cerinţele guvernării democratice. Cum va fi influenţată

activitatea din acest domeniu – o activitate guvernamentală ce are ca funcţii principale culegerea, protejarea şi transmiterea informaţiilor – de aspectele privind disponibilitatea şi transmiterea informaţiilor – iată ce încercăm să urmărim în a treia ediţie a lucrării de faţă.

Deşi *Războiul tăcut* a fost revizuită şi adusă la zi de două ori până acum, subiectul, structura şi conţinutul de bază ale cărţii au rămas neschimbate. *Războiul tăcut* nu este o prezentare istorică a activităţii de informaţii desfăşurate de un anumit guvern. Cu toate că majoritatea exemplelor folosite în carte sunt preluate din experienţa serviciilor britanice şi americane, rolul lor este de a prezenta concepte generale şi chestiuni ce definesc activitatea de informaţii. Sfârşitul Războiului Rece, debutul unei noi ere strategice şi riscurile aduse de „era informaţională" vor determina, evident, schimbări la nivelul practicilor şi solicitărilor ce ţin de serviciile de informaţii. Însă ceea ce-şi propune să demonstreze lucrarea de faţă este faptul că lumea informaţiilor este strâns legată de concurenţa dintre state şi că, în lipsa acelei stări de „pace perpetuă" atât de dragă lui Kant, informaţiile rămân, alături de diplomaţie şi forţele militare, instrumente de guvernare. În acest sens, atât cetăţeanul, cât şi studentul trebuie să înţeleagă că elementele de bază ale activităţii de informaţii, interacţiunile, tensiunile şi relaţia uneori dificilă dintre servicii şi guvernul democratic, precum şi dintre servicii şi societate au ca scop final îmbunătăţirea securităţii.

La ediţia aceasta, ca şi la cele anterioare, au contribuit şi au adus completări, precizări şi comentarii numeroşi studenţi, prieteni şi colegi. Mulţumiri lui Eliot A. Cohen, Kenneth E. de Graffenreid, Hillel G. Fradkin, Sam Halperin, Sheila Kerr, Carnes R. Lord, Kenneth G. Robertson şi Diane S. Roark. Prima ediţie a cărţii a fost scrisă în perioada în care lucram la Naţional Strategy Information Office (NSIC), când am beneficiat de granturile Fundaţiei John M. Olin şi ale Fundaţiei Lynde şi Harry Bradley. A doua ediţie a fost revizuită de Gary, care este senior fellow al NSIC. Mulţumiri speciale lui Roy Godson, preşedintele NSIC, şi lui Jeffrey Berman, director al NSIC.

*Abram N. Shulsky Washington, DC*

## Către cititor

Nu s-a făcut nicio revizuire a textului în urma atacurilor teroriste din 11 septembrie 2001, moment în care lucrarea noastră era deja gata de tipar. Sigur, va trece mult timp până când se vor vedea implicaţiile acestor evenimente. Totuşi, este evident că se va acorda mai multă atenţie culegerii de informaţii din surse umane în vederea contracarării unor potenţiale atacuri teroriste; în special, se va pune tot mai mult accent pe acoperirea „neoficială” a ofiţerilor de informaţii. Legile privind securitatea internă se vor diversifica, iar chestiunile privind interceptările şi supravegherea operativă vor deveni subiecte de interes din perspectiva întrebării dacă grupurile şi indivizii pot fi supuşi monitorizării în baza unei decizii politice, chiar dacă nu există nicio dovadă a comiterii unei infracţiuni.

## Introducere

A scrie despre secrete în cursul ultimului sfert de secol, serviciile de informaţii – în ciuda faptului că una dintre trăsăturile lor esenţiale rămâne caracterul secret – au început să fie tot mai des prezente în presă şi să facă obiectul a numeroase studii şi cercetări ştiinţifice. Dezbaterile şi întrebările despre serviciile de informaţii nu mai constituie doar motiv de scandal şi discuţii în contradictoriu. Acestea au fost acceptate ca un aspect normal al dezbaterilor publice privind activităţile guvernamentale în genere.

Deşi dezbaterile publice despre evenimentele obişnuite din domeniul culegerii de informaţii depind în continuare, în mare măsură, de materialul brut privind „scurgerile" autorizate sau neautorizate de informaţii clasificate, numărul lucrărilor pe această temă a crescut. Odată cu trecerea timpului, amplificată de o mai mare deschidere din partea multor guverne democratice, au fost făcute publice multe din materialele istorice legate de al Doilea Război Mondial şi de Războiul Rece. În plus, căderea comunismului în fosta Uniune Sovietică şi în Europa de Est a făcut posibil accesul la anumite arhive, în special cele din fosta RDG şi, în mai mică măsură, în Rusia. Abordarea „dimensiunii" *intelligence* devine o practică standard în ce priveşte, în special, istoria diplomatică şi militară.

Intensificarea dezbaterilor publice pe probleme privind culegerea de informaţii în

general nu a condus totuşi la o mai bună înţelegere a acestui domeniu. Într-adevăr, dezbaterile publice recente privind culegerea de informaţii sunt caracterizate de o neglijare a întrebărilor fundamentale despre rolul pe care trebuie să îl aibă serviciile de informaţii şi caracterul secret într-o democraţie. Într-un sens mai general, exceptând câteva lucrări de specialitate care au coincis cu ultima încercare majoră a Congresului american de a „reforma" serviciile de informaţii (la începutul anilor '90), abordarea publică a aspectelor legate de culegerea de informaţii, atunci când nu au avut nicio încărcătură istorică, a fost similară abordării specifice cazurilor de spionaj.

Aceasta contrastează cu valul de lucrări privind domeniul culegerii de informaţii din anii '70 şi începutul anilor '80. În acea perioadă, mare parte a dezbaterilor publice privind serviciile – mai ales în Statele Unite, dar cu ecouri şi în alte ţări democratice – putea fi catalogată ca aparţinând uneia dintre cele două tabere care se diferenţiau prin abordările lor faţă de ideea fundamentală privind rolul serviciilor de informaţii într-o societate democratică şi relaţia dintre caracterul secret şi normele guvernării democratice.

Potrivit uneia dintre tabere, serviciile de informaţii au devenit sau, cel puţin, ar fi trebuit să devină mai puţin nişte instituţii „de capă şi spadă" şi mai curând să se constituie într-o sferă a ştiinţelor sociale care să caute să analizeze şi în final să anticipeze problemele de natură politică,

economică, socială şi militară. Prin urmare, nu era nevoie să desfăşoare o activitate prin definiţie secretă. Dacă pentru a proteja sursele unor informaţii importante caracterul secret este necesar, aspectele esenţiale privind mişcările politice, economice, sociale, tehnologice şi demografice care conturează direcţia în care se îndreaptă un stat pe termen lung nu ar trebui să constituie un mare secret!1 Astfel, nu numai că problemele privind domeniul informaţiilor ar putea fi dezbătute public fără dificultate, ci, prin demistificarea acestui domeniu şi încurajarea schimbului de idei între comunităţile de informaţii şi cele academice, dezbaterile publice ar putea ajuta serviciile de informaţii să-şi atingă şi chiar să-şi depăşească scopul de a deveni o ştiinţă socială (serviciile de informaţii devenind, mai curând, „grupuri consultative de experţi”) 2.

Potrivit celeilalte tabere, articolele despre culegerea de informaţii au ca scop dezvăluirea de eventuale ilegalităţi şi erori, precum şi îmbunătăţirea modului în care operează agenţiile3. Din această perspectivă, secretul care învăluia operaţiunile serviciilor secrete a fost fie cauza unor ilegalităţi, fie o precondiţie necesară a acestora. Prin urmare, dezbaterile publice pe marginea problemelor privind culegerea de informaţii au constituit un remediu în sine. Indiferent ce prejudiciu ar fi adus dezvăluirea unor secrete legitime, acest lucru era considerat nesemnificativ comparativ cu prejudiciile pe care le-ar putea aduce serviciile secrete însele, operând fără ştirea publicului. Aşadar, dezvăluirea

anumitor informaţii despre un serviciu secret „nereformat” nu constituia o problemă – deşi s-ar fi găsit voci care să afirme că, departe de privirile opiniei publice, orice astfel de organizaţie se poate abate de la scopurile ei iniţiale.

În ultima perioadă, majoritatea studiilor şi cercetărilor în domeniu s-au axat pe relatări istorice privind activităţile specifice de culegere a informaţiilor4. Dezbaterile pe marginea mai multor aspecte curente au fost dominate de relatarea unor cazuri de spionaj, accentul punându-se mai degrabă pe acuzaţiile de incompetenţă decât pe abuzurile de natură etică sau politică5. Aceste lucrări nu aveau tendinţa de a susţine anumite idei politice sau ideologice (în afară de faptul evident, se pare, că este mai bine să avem un serviciu de informaţii competent decât unul incompetent).

*Războiul tăcut* îşi propune să dea răspunsuri la o serie de întrebări, încearcă să abordeze conceptele fundamentale în înţelegerea lumii serviciilor de informaţii. Scopul este de a-i da cititorului posibilitatea să mediteze la aspectele generale ale politicii de culegere a informaţiilor astfel încât să înţeleagă complexitatea şi ambiguităţile inerente acestei sfere de activitate. De aceea, abordarea este una fundamental teoretică; pentru a ilustra aspectele generale sunt utilizate detalii cunoscute despre activitatea reală a serviciilor de informaţii6; nu se face nicio încercare de înţelegere a trecutului serviciilor sau a statutului lor actual.

Acesta este motivul pentru care volumul se

poate baza pe informaţiile publice privind activităţile de culegere a informaţiilor7. Nu au existat niciun fel de încercări de furnizare a unor informaţii care să nu fie deja cunoscute publicului. Acest lucru se datorează, în parte, faptului că am primit drept de acces la informaţii secrete ce priveau diferite poziţii din cadrul conducerii Statelor Unite (totuşi, nu şi din cadrul vreunui serviciu secret). Ca o precondiţie a dreptului de acces, am promis să nu dezvăluim astfel de informaţii8.

Ce este şi mai important, considerăm confidenţialitatea esenţială în operaţiunile de *intelligence* şi, în orice caz, nu credem că publicarea unor amănunte despre misiunile serviciilor secrete americane este necesară. Majoritatea acestor detalii nu par să ridice probleme importante de politici publice sau să fie necesare pentru înţelegerea conceptelor fundamentale de culegere a informaţiilor pe care le avem în vedere în prezenta carte.

Deşi culegerea de informaţii devine un domeniu de studiu ştiinţific recunoscut, mai ales în lumea occidentală, teoretizarea pe marginea acestuia rămâne într-un stadiu incipient. Prin această carte încercăm să diminuăm acest neajuns. În acelaşi timp, trebuie să admitem că, raportându-se în mare parte la experienţa anglo-americană, această carte este departe de a oferi o „teorie a culegerii de informaţii" general-valabilă. Această raportare se datorează în mare parte faptului că majoritatea informaţiilor publice despre acest tip de activităţi se referă, deloc

surprinzător, la serviciile secrete ale acelor ţări care dispun de cele mai deschise sisteme politice. Cu toate acestea, acolo unde este posibil, facem referire şi la activităţile serviciilor secrete ale altor ţări şi ne punem problema diferenţelor dintre aceste servicii, determinate de natura regimurilor pe care le servesc.

Prezenta carte nu le dezvăluie cititorilor niciun fel de secrete sau „informaţii din interior”, fie ele spectaculoase sau lipsite de interes. Sperăm să oferim, în schimb, elementele necesare înţelegerii domeniului în sine, precum şi multe picanterii care, fără îndoială, vor continua să ajungă la urechile publicului.

## Capitolul 1

## Ce este activitatea de informaţii?

În romane şi în imaginaţia publicului, domeniul informaţiilor a fost foarte des asociat cu spionajul şi comportamentul fără scrupule, cu şantajul sexual al unei Mata Hari şi acţiunile „de capă şi spadă” ale lui James Bond. Deşi activităţile de acest tip au o anumită pondere în domeniul informaţiilor, conceptul este mult mai larg. Pentru a surprinde această complexitate, putem începe prin analizarea diferitelor categorii de fenomene cărora li se aplică termenul *intelligence*; acestea includ anumite *informaţii*, *activităţi* şi *organizaţii1*.

Este vorba despre *informaţiile* relevante pentru formularea şi implementarea unei politici guvernamentale în scopul promovării intereselor sale de securitate naţională şi al prevenirii ameninţărilor din partea unor adversari reali sau potenţiali. (Termenul *adversar* este folosit aici într-un sens larg. De exemplu, un guvern-prieten, cu care se negociază un tratat, poate fi *adversar în contextul negocierilor*; se presupune că părţile intră în competiţie pentru a maximiza beneficiile pe care le obţin în urma acordului, cel puţin într-o anumită măsură pe cheltuiala celeilalte.) în cele mai clare şi adesea cele mai importante cazuri, aceste informaţii se referă la aspecte din domeniul militar, cum ar fi capacităţile adversarului şi planurile pentru o acţiune militară. Inamicii reali sau potenţiali, în general, îşi dau toată silinţa să ţină secrete aceste informaţii. Desigur, alte tipuri

de informaţii secrete pot fi la fel de importante – de exemplu, datele referitoare la activităţile şi intenţiile diplomatice ale altei ţări, precum şi la activităţile acesteia în domeniul informaţiilor.

Pe lângă datele de acest tip, cunoaşterea multor altor tipuri de informaţii referitoare la un adversar real sau potenţial poate fi folositoare, chiar dacă adversarul nu intenţionează să le ţină secrete. Acestea se pot referi la politica internă şi la dezvoltarea societăţii, precum şi la statisticile economice şi demografice. Câte din aceste date sunt publice depinde de natura regimului politic. Într-o societate democratică, ele sunt aproape întotdeauna accesibile publicului. Un sistem autoritar sau totalitar, dimpotrivă, încearcă deseori să ascundă orice informaţii referitoare la politica sa internă, situaţia economică sau tendinţele sociale pe care un adversar le-ar considera utile. Indiferent cât de multe din informaţiile publice („din surse deschise”) ar trebui, în sens strict, să fie considerate „informaţii secrete”, trebuie neapărat să aibă loc un proces prin care să fie puse în mod sistematic la dispoziţia oficialilor guvernamentali într-o formă utilizabilă. Un serviciu de informaţii preia deseori această activitate.

Informaţiile nu includ numai „materialul brut” cules prin metode de spionaj sau în alt mod, ci şi analize şi evaluări care se bazează pe ele. Acest rezultat, denumit şi „produs” informativ, are o importanţă deosebită pentru strategi. Proporţia în care acest produs informativ face posibilă prezentarea unei evaluări exhaustive a situaţiei,

bazându-se pe toate datele disponibile, atât publice, cât şi secrete, variază de la un serviciu de informaţii la altul.

Ca *activitate*, acest domeniu presupune culegerea şi analizarea informaţiilor. De asemenea, include acţiunile întreprinse pentru a contracara activităţile informative ale adversarilor, fie neacordându-le acces la informaţii, fie inducându-i în eroare cu privire la unele fapte şi semnificaţia acestora.

Domeniul informaţiilor cuprinde o gamă largă de activităţi. De exemplu, există metode diverse de culegere a informaţiilor, precum spionajul, fotografierea aeriană, interceptarea comunicaţiilor şi studierea documentelor publice disponibile, programe de radio şi televiziune, precum şi resursele disponibile pe Internet. Există, de asemenea, tehnici diferite pentru analizarea informaţiilor care au fost culese: unele dintre acestea pot fi similare metodelor pe care le folosesc ştiinţele sociale, iar altele, precum decodarea mesajelor codificate, sunt caracteristice domeniului informaţiilor. În mod similar, ascunderea informaţiilor faţă de alţii implică diverse activităţi unele dintre acestea fiind similare cu cele care au ca scop aplicarea legii, precum investigarea şi urmărirea agenţilor străini suspecţi pentru a afla ce fel de activităţi desfăşoară aceştia. Altele sunt mai esoterice, precum folosirea unor coduri pentru a proteja comunicaţiile (deşi progresele recente înregistrate în domeniul tehnologiei informaţiei au dus la crearea unor instrumente de codificare care pot fi

comercializate). De asemenea, există metode diferite de inducere în eroare a adversarilor, precum operaţiuni de tip „agent dublu” şi transmiterea unor mesaje false (aceasta înseamnă transmiterea unor mesaje de inducere în eroare care anticipează faptul că adversarul le va intercepta şi le va da crezare).

Datorită acestei varietăţi de activităţi, pare dificil de găsit un punct comun care să le relaţioneze. Toate acestea au legătură cu obţinerea sau contestarea informaţiilor. De aceea, culegerea de informaţii ca activitate poate fi definită drept componentă a luptei dintre adversari care folosesc în primul rând informaţiile (spre deosebire, de exemplu, de competiţia economică, manevrele sau negocierile diplomatice, ameninţările ori folosirea forţei militare).

În fine, termenul *informaţii* se referă, de asemenea, la o *organizaţie* care efectuează aceste activităţi. Una dintre principalele caracteristici ale unor astfel de organizaţii este confidenţialitatea cu care trebuie coordonate aceste activităţi. Multe dintre metodele lor de operare, precum folosirea agenţilor sub acoperire sau a regulilor stricte privind accesul la informaţii, sunt rezultatele acestei condiţii. Deoarece agenţiile de informaţii sunt organizate pentru a îmbunătăţi capacitatea de asigurare a confidenţialităţii, acestora li se poate atribui, împreună cu funcţiile privind informaţiile, responsabilitatea efectuării activităţilor secrete pentru a promova obiectivele de politică externă ale guvernelor lor mai direct.

O astfel de activitate, denumită „acţiune secretă” în terminologia din domeniul informaţiilor în SUA, poate cuprinde de la aspecte banale, precum asistarea în mod secret a unui guvern străin prieten, până la aspecte spectaculoase, precum orchestrarea răsturnării acelora ostile. Întrebarea dacă acestea ar trebui să intre în atribuţiile aceloraşi organizaţii care culeg şi analizează informaţii a reprezentat un aspect uneori controversat. Chiar dacă, din motive birocratice, serviciilor de informaţii li se atribuie responsabilitatea pentru acţiunile secrete, rămâne problema fundamentală – din punct de vedere teoretic şi practic – dacă acţiunea secretă ar trebui considerată ca făcând parte din domeniul informaţiilor.

## Delimitarea domeniului

Deoarece nu numai guvernele, ci şi alte tipuri de organizaţii acţionează într-un mediu caracterizat de competitivitate, conceptul de *servicii de informaţii* poate fi aplicat şi în cazul acestora. De exemplu, unii cercetători extind conceptul şi asupra corporaţiilor de afaceri, considerând că implică „informaţii organizate… menite să satisfacă nevoile strategice unice ale unei întreprinderi” 2. În mod similar, se poate vorbi despre o activitate de culegere de informaţii în cadrul unui partid politic sau al unei campanii, în încercarea de a afla ce plănuieşte opoziţia.

Aceste posibile extinderi ale sensului sintagmei *serviciu de informaţii* nu sunt discutate

în acest volum, care se limitează la obiectivele tradiţionale ale domeniului informaţiilor – adică la informaţii şi activităţi relevante pentru problemele de securitate naţională ale guvernelor.

Dar, chiar şi acceptând această limitare, obiectivul domeniului informaţiilor rămâne neclar într-o anumită măsură, de vreme ce sintagma *securitate naţională* este ea însăşi nedefinită. Sensul său de bază se referă la protejarea naţiunii împotriva ameninţărilor, în ultimă instanţă militare, reprezentate de naţiuni străine. Atunci când o naţiune este invadată sau este pe punctul de a fi atacată, problemele sale de securitate se concentrează în mod clar asupra apărării sau prevenirii invadării şi asupra prevenirii unor situaţii similare pe viitor. În perioade mai paşnice, poate fi mai puţin clar ce naţiuni străine, evenimente sau circumstanţe ameninţă securitatea naţională şi de aceea este necesară atenţia agenţiilor de informaţii ale ţării respective3.

Problema se complică şi mai mult prin faptul că interesele de securitate naţională şi deci ameninţările la adresa lor nu pot fi independente de tipul de guvernare a ţării (sau regim) şi de concepţiile ideologice. Deşi susţinătorii *Realpolitik* ar argumenta că interesele unei naţiuni sunt determinate de factorii obiectivi ai sistemului internaţional, vederile ideologice şi în general cultura politică a ţării influenţează modul în care le percepe un guvern4. De exemplu, caracterul ideologic al unui regim poate stabili dacă acesta consideră o anumită ţară străină drept o

ameninţare. În special, puterile statu-quo şi cele revoluţionare au de obicei păreri diferite despre ceea ce constituie o ameninţare la adresa securităţii naţionale.

Informaţiile interne

Un aspect şi mai important în care natura regimului afectează obiectivul domeniului informaţiilor îl constituie „informaţiile interne”. Orice guvern trebuie să fie preocupat nu numai de ameninţările externe (precum invazia militară), ci şi de ameninţările la adresa capacităţii sale de guvernare sau chiar a existenţei sale care vin din partea unor indivizi sau grupuri din interiorul graniţelor. Astfel de ameninţări ar putea veni din partea unor grupuri care încearcă să răstoarne guvernul prin mijloace ilegale, prin folosirea violenţei în scopul schimbării politicii de guvernare sau prin excluderea din organismul politic a unor membri aparţinând unei anumite etnii, rase sau unui grup religios. Dar modul în care un guvern defineşte astfel de ameninţări interne depinde în mare măsură de tipul de guvernare care există.

Un regim în care o dinastie sau un singur partid politic deţin monopolul asupra puterii, de exemplu, probabil consideră orice disensiune internă politică drept o ameninţare la adresa securităţii, iar serviciul de informaţii se va concentra asupra detectării şi îndepărtării acelei disensiuni. În cazuri extreme, guvernul unui stat totalitar poate considera toate persoanele care nu fac parte din partidul de guvernare drept actuali sau potenţiali duşmani 5. Spre deosebire de

aceasta, noţiunea de *oponenţi loiali*, care se regăseşte în sistemele parlamentare sau alte sisteme democratice, implică faptul că oponenţii politici pe plan intern ai guvernului nu reprezintă ameninţări la adresa securităţii şi de aceea nu sunt ţinte ale serviciilor de informaţii.

În plus, grupările interne care sunt ostile nu numai guvernului în funcţie, ci şi sistemului fundamental de guvernare a naţiunii (sau regimului) pot intra în relaţii cu puteri străine în diferite moduri. La un capăt al spectrului extern-intern va fi un individ sau un grup care acţionează în numele şi în direcţia unei puteri străine ostile. Ar putea exista, de asemenea, grupuri sau indivizi care împărtăşesc obiective comune cu o putere străină şi cooperează pentru realizarea scopurilor lor. Ar putea exista grupări care împărtăşesc convingeri ideologice sau de altă natură cu un adversar străin, dar care nu au practic legături cu acesta. Regimuri diferite pot avea păreri diverse cu privire la tipul de grupare ce reprezintă o ameninţare la adresa securităţii naţionale, trebuind culese informaţii.

## Serviciile de informaţii şi aplicarea legii

O problemă asociată este reprezentată de ameninţările denumite „transnaţionale”, care nu sunt generate în primul rând de un guvern străin, de exemplu, traficul de droguri, terorismul internaţional sau anumite tipuri de crimă organizată. Acestea pot reprezenta ameninţări serioase la adresa bunăstării unei naţiuni, dar

sunt mai degrabă responsabilitatea organismelor însărcinate cu aplicarea legii, nu a serviciilor de informaţii. Totuşi, serviciile de informaţii sunt adesea implicate în lupta împotriva lor, din mai multe motive. În primul rând, acestea implică activităţi pe teritoriul unor ţări străine, unde organismele însărcinate cu aplicarea legii dintr-un anumit stat nu sunt abilitate să acţioneze, iar cele din ţările respective nu sunt capabile sau nu doresc să ofere asistenţă. Serviciile de informaţii pot fi solicitate pentru informaţii referitoare la caracteristicile externe ale acestor activităţi, informaţii care nu ar fi disponibile în alt mod.

În al doilea rând, din perspectiva aplicării legii, de obicei se aşteaptă până când o infracţiune a fost sau este pe punctul de a fi săvârşită şi de-abia atunci se încearcă rezolvarea cazului respectiv, precum şi arestarea infractorilor. Aceasta ar putea să nu fie o abordare adecvată în ceea ce priveşte anumite ameninţări transnaţionale. Un singur incident, precum declanşarea unei bombe într-un avion de pasageri în timpul zborului, poate cauza pagube atât de mari, încât un guvern trebuie să încerce să prevină astfel de incidente, şi nu să le rezolve după ce s-au produs. Mai mult decât atât, o anumită infracţiune, cum ar fi un simplu caz de contrabandă cu narcotice, poate fi doar o parte din cadrul unor operaţiuni ale unei organizaţii criminale; dacă aceasta este mare şi bine organizată, arestarea unor infractori care au comis o singură infracţiune poate să nu aibă un impact prea puternic. Astfel de arestări ocazionale

pot reprezenta, din perspectiva liderilor, un preţ acceptabil pentru derularea afacerii. Chiar dacă agenţiile se mulţumesc să aştepte până când se comite o anumită infracţiune, şansele de rezolvare a cazului depind foarte mult de informaţiile disponibile referitoare la organizaţia implicată.

Din aceste motive, guvernele adoptă adesea o abordare informativă specifică acestor tipuri de activităţi. În loc să aştepte comiterea unei anumite infracţiuni asupra căreia să se concentreze, agenţiile adună informaţii timp îndelungat cu privire la anumiţi indivizi şi la anumite grupări – motivaţiile lor, resursele, interconexiunile, intenţiile şi aşa mai departe. Se impune adesea folosirea unor informatori, care se infiltrează în grupările implicate şi operează asemenea spionilor. Este posibil, de asemenea, să fie interceptate comunicaţiile sau să fie folosite alte metode tehnice pentru culegerea de informaţii. De aceea, serviciile de informaţii sunt deseori implicate în lupta împotriva grupărilor transnaţionale. În funcţie de regim, implicarea agenţiilor poate fi limitată la caracteristicile externe ale activităţilor lor, în timp ce aspectele interne rămân în atribuţiile organismelor însărcinate cu aplicarea legii.

Chiar şi în abordarea problemei reprezentate de grupurile de crimă organizată care acţionează exclusiv pe plan intern, organismele însărcinate cu aplicarea legii folosesc adesea tehnici specifice serviciilor de informaţii. De exemplu, în ceea ce priveşte menţinerea legii pe plan intern, Biroul Federal de Investigaţii din SUA (FBI) face

distincţia între anchetele penale secrete şi anchetele penale obişnuite. Dintre acestea două, primul tip de investigaţii este descris ca „mai extins şi mai puţin discriminator decât cel obişnuit”; acesta nu se concentrează asupra săvârşirii unei singure acţiuni infracţionale, ci asupra unei organizaţii criminale, fiind necesară stabilirea dimensiunii şi structurii acesteia, a acţiunilor sale trecute, a intenţiilor criminale şi a capacităţii de a produce daune7. Diferenţa dintre abordarea bazată pe aplicarea legii şi cea a serviciilor de informaţii este reprezentată de concentrarea atenţiei asupra pedepsirii unei anumite acţiuni criminale sau asupra luptei cu o organizaţie implicată într-o activitate criminală.

## Economia şi activitatea de informaţii

Există întrebări referitoare la modul de funcţionare al serviciilor de informaţii în ceea ce priveşte problemele economice. Din nou, multe lucruri depind de natura regimului şi de sistemul economic al ţării, într-un sistem cu o economie coordonată de guvern, domeniul informaţiilor se va concentra asupra aspectelor economice privind relaţiile guvernului respectiv cu alte guverne (precum comerţul internaţional) în aceeaşi măsură ca şi toate celelalte aspecte ale relaţiilor internaţionale, în plus, serviciile de informaţii pot fi folosite pentru a creşte bunăstarea economică a statului. Achiziţionarea unei tehnologii occidentale avansate, de exemplu, a reprezentat o sarcină importantă a serviciilor de informaţii ale Uniunii

Sovietice (şi rămâne un obiectiv important al serviciilor de informaţii rus şi chinez). Această activitate nu numai că a ridicat nivelul tehnologic al Armatei sovietice sau chineze, ci a şi scutit ambele ţări de cheltuielile mari şi de dificultatea de a dezvolta o tehnologie proprie, fie în scop militar, fie civil8.

Într-o economie de piaţă, nu este foarte clar care sunt aspectele economice importante pentru securitatea naţională care justifică sau presupun implicarea serviciilor de informaţii. Există un număr de domenii specifice, precum evaluarea capacităţii economice a unui potenţial adversar militar sau progresele ulterioare care afectează fluxul de resurse vitale strategice, asupra cărora guvernele pot cere informaţii detaliate. Angajarea agenţiilor şi folosirea metodelor de culegere a informaţiilor depind într-o oarecare măsură de încercarea statelor respective de a le ţine sau nu secrete. În general, problemele economice specifice cu impact direct asupra aspectelor legate de securitatea naţională care privesc politica militară sau externă intră în responsabilitatea serviciilor de informaţii. De exemplu, pe timp de război, metodele serviciilor de informaţii pot fi folosite pentru a obţine acces la materiale strategice (sau pentru a induce în eroare adversarii astfel încât să nu aibă acces la acestea), un obiectiv-cheie al securităţii naţionale. În mod similar, în decursul negocierilor cu o ţară străină pe probleme economice, o naţiune îşi poate folosi resursele secrete pentru a afla care sunt avantajele pe care ar urma să le obţină partenerii

în urma negocierilor.

Interesul manifestat de un stat cu privire la informaţiile de natură economică legate de activitatea industrială, comercială sau financiară a altor state depinde probabil de posibilitatea ca guvernul acestuia să aibă o birocraţie a „strategiei industriale” care să folosească aceste informaţii. Ca urmare, problemele legate de folosirea serviciilor de informaţii pentru a culege date economice reprezintă într-o mare măsură surogate pentru o dezbatere fundamentală privind rolul guvernului în direcţionarea viitorului economic al unei ţări.

Întrebarea mai generală este totuşi dacă ar trebui folosite metodele informative pentru creşterea bunăstării economice a unei naţiuni9. Deoarece încheierea Războiului Rece a redus riscul unei confruntări militare între principalele puteri, forţa economică a început să câştige o poziţie importantă în stabilirea puterii şi a prestigiului internaţionale ale unei ţări; în consecinţă, a crescut interesul pentru rolul pe care serviciile de informaţii îl puteau juca în consolidarea situaţiei economice10. Situaţia economică a unei naţiuni se îmbunătăţeşte sau se degradează în timp din cauza unor factori precum coeficientul de investiţii, productivitatea muncii, aptitudinile de management şi nivelul de educaţie al forţei de muncă. În plus, deşi unele evoluţii din economia internaţională pot avea importante consecinţe pentru securitatea naţională, nu este clar dacă guvernul ar trebui sau dacă ar putea să facă prea multe în privinţa acestor progrese. Mai

mult decât atât, într-o societate democratică, politica economică pare a fi mai degrabă determinată de interacţiunile intereselor economice pe plan intern decât de vreo viziune coerentă (bazată sau nu pe informaţii) a unei viitoare situaţii economice mondiale. Din aceste motive, nu este clar dacă un guvern precum cel al Statelor Unite ar fi un consumator important de asemenea informaţii. Acestea ar putea servi interesele economice, dar nu este clar dacă informaţiile culese clandestin pe cheltuiala guvernului ar fi distribuite echitabil unor indivizi sau corporaţii pentru interese private ulterioare".

Alte aspecte „netradiţionale".

Unii cercetători ai acestui domeniu au afirmat că pe lângă aspectele economice mai există şi preocupări „netradiţionale" care trebuie considerate ca intrând în sarcina serviciilor de informaţii – de exemplu, probleme referitoare la mediu. Deşi există argumente conform cărora problemele de mediu pot afecta securitatea naţională, motivul principal pare a fi că sistemele tehnice de culegere a informaţiilor dezvoltate în alte scopuri pot să ajute la urmărirea schimbărilor de mediu de-a lungul timpului şi pe zone extinse şi să facă aceasta cu costuri suplimentare scăzute12.

Serviciile secrete şi era informaţională

Ţinând cont de faptul că serviciile secrete lucrează cu informaţii, este corect să presupunem că acestea vor fi afectate serios de apariţia a ceea ce a primit numele „era informaţională". Noţiunea de *eră informaţională* este destul de ambiguă. Totuşi, în mod clar este foarte importantă; deja a

schimbat modul în care multe organizaţii operează – în special corporaţiile din domeniul afacerilor – şi probabil va avea efecte importante asupra guvernului.

Din punct de vedere tehnic, factorul coordonator este progresul tehnologic extraordinar care s-a înregistrat în procesarea şi comunicarea informaţiilor. Schimbarea tehnologică reprezintă doar o mică parte a întregii imagini: mai importante sunt schimbările de comportament şi instituţionale determinate de concentrarea asupra informaţiilor-cheie pentru activitatea organizaţională. (în domeniul militar, ceea ce este adesea denumit „revoluţia în afacerile militare" depinde foarte mult de utilitatea sporită a informaţiilor prin selectarea unor noi tipuri de arme de precizie şi prin întărirea capacităţii de a culege, a procesa şi a disemina acele informaţii într-un timp scurt în scop operaţional.)

Efectul acestor schimbări este resimţit în diverse forme. La un nivel, acestea sugerează noi moduri în care informaţiile pot fi transferate mai rapid şi folosite în cadrul guvernului, astfel încât formularea şi implementarea politicilor să fie mai eficiente. În plus, schimbările decurg ca urmare a concentrării unei cantităţi mari de informaţii disponibile pentru întreaga societate, atât la nivelul unor departamente guvernamentale, care nu fac parte din serviciile de informaţii, cât şi al unor entităţi din afara guvernului. Cu alte cuvinte, serviciile de informaţii consideră că alte tipuri de organizaţii devin mai eficiente în culegerea,

analizarea şi transmiterea datelor – aceasta înseamnă că serviciile de informaţii au, în ceea ce priveşte unele tipuri de date, o „concurenţă” mai mare în transmiterea lor către factorii de decizie. Din perspectiva guvernului, este important să fie găsită o modalitate cât mai eficientă de exploatare a datelor generate şi de transmitere a acestora oriunde în societate, precum şi să existe siguranţa că produsul unic al serviciilor de informaţii este combinat cu alte surse într-un mod care să răspundă cel mai bine nevoii de informare a guvernului13.

Elementele activităţii serviciilor de informaţii

Indiferent de raza de acţiune, activităţile serviciilor de informaţii pot li clasificate în patru categorii, menţionate de obicei ca fiind „componente ale domeniului informaţiilor”: *culegerea*, *analiza*, *acţiunile secrete/sub acoperire* şi *contrainformaţiile*. Deoarece aceste elemente sunt analizate în detaliu în următoarele capitole, ne propunem în continuare doar să clarificăm natura celor patru tipuri de activităţi ale serviciilor de informaţii şi schiţarea relaţiilor dintre acestea.

*Culegerea* se referă la adunarea datelor brute, prin spionaj, metode tehnice (fotografiere, interceptarea comunicaţiilor electronice şi alte metode care implică tehnologia), exploatarea „surselor deschise” (de exemplu, publicaţiile, emisiunile de radio şi televiziune) sau prin orice alte metode. În timp ce culegerea este în mod clar esenţială în activitatea serviciilor de informaţii, există opinii diferite în ceea ce priveşte

importanţa relativă a diferitelor metode. De exemplu, unii cercetători ai domeniului au dezbătut importanţa relativă a culegerii de informaţii din „surse deschise” comparativ cu metodele caracteristice serviciilor de informaţii, precum şi cea a spionajului comparativ cu folosirea mijloacelor tehnice.

Indiferent cât de valoroase sunt informaţiile culese, aproape niciodată acestea nu sunt suficient de clare. Cu alte cuvinte, este necesară o analiză a informaţiilor pentru a fi de folos factorilor de decizie şi comandanţilor militari. În majoritatea cazurilor, informaţiile culese sunt fragmentare, ambigue şi susceptibile de interpretări divergente. De aceea, procesul analizării informaţiilor disponibile în scopul emiterii de judecăţi referitoare la capacităţile, intenţiile şi acţiunile altei părţi reprezintă o componentă vitală a acestui proces. Şi mai dificil este procesul de anticipare („estimare”, în jargonul serviciilor secrete americane) a capacităţilor viitoare, intenţiilor şi acţiunilor unui guvern străin sau ale unei organizaţii politice.

În plan conceptual, *acţiunea secretă*/*sub acoperire* diferă de alte componente ale domeniului în sensul că, în timp ce altele se concentrează asupra căutării şi protejării informaţiilor, acţiunile sub acoperire urmăresc să influenţeze în mod direct evenimentele politice, în ceea ce priveşte intensitatea, acţiunea sub acoperire poate varia de la persuasiune sau propagandă la acţiuni paramilitare; a fost descrisă ca „o activitate la limita dintre diplomaţie şi

război” 14.

Deşi tehnicile de exercitare a influenţei sunt numeroase, ele au atributul comun al anonimatului – rolul guvernului în coordonarea activităţii nu este vizibil sau cunoscut public. Din acest motiv, capacitatea unui serviciu de informaţii de a acţiona în secret presupune de cele mai multe ori că poate derula şi acţiuni secrete. Dar, după cum am afirmat mai sus, deoarece această activitate implică mai degrabă implementarea unei strategii decât informarea factorilor de decizie, în Statele Unite s-a sugerat de multe ori ca acţiunile secrete să nu fie derulate de aceeaşi agenţie (adică CIA) care culege şi analizează informaţiile secrete. Totuşi, atât în Statele Unite, cât şi în Marea Britanie experienţa anterioară a arătat că având două agenţii care coordonează operaţiuni clandestine (una pentru spionaj şi cealaltă pentru acţiuni sub acoperire) se poate ajunge la o rivalitate epuizantă, dublarea efortului şi imixtiuni15.

În sensul cel mai general, *conârainformaţiile* caută să protejeze societatea (şi în special capacităţile sale din domeniul informaţiilor) împotriva oricăror ameninţări din partea unor servicii de informaţii ostile. În primul rând, contrainformaţiile implică inducerea în eroare a adversarilor. Această protecţie este realizată prin programe de securitate (acţiuni întreprinse pentru ca informaţiile să nu ajungă la cei neautorizaţi) şi prin contraspionaj (acţiuni întreprinse pentru a reţine sau a neutraliza agenţii străini, astfel încât să se prevină obţinerea şi comunicarea de către

aceştia a informaţiilor secrete). În plus, contrainformaţiile pot încerca să ofere protecţie împotriva posibilităţilor adversarului de a culege informaţii şi de a le analiza; aceasta se realizează prin operaţiuni de dezinformare ce furnizează date false sau intenţionat eronate pentru a determina adversarul să ajungă la concluzii incorecte cu privire la capacităţile, acţiunile sau intenţiile cuiva.

Protejarea împotriva capacităţilor de informare ale unui adversar, în sens larg, presupune şi alte activităţi. Poate fi necesară parcurgerea anumitor etape pentru a evita dezinformarea provocată de furnizarea deliberată de date eronate de către cealaltă parte. De aceea, contrainformaţiile trebuie să protejeze integritatea funcţiilor de culegere şi analiză a datelor. De asemenea, este importantă cunoaşterea acţiunilor secrete întreprinse de un guvern străin în scopul influenţării guvernului sau societăţii unei ţări. În sfârşit, sfera activităţilor de contrainformaţii este determinată de ameninţarea reprezentată de activităţile serviciilor de informaţii ale adversarului.

Capitolul 2

Spioni, maşini şi biblioteci: culegerea informaţiilor începem discuţia privind elementele activităţii serviciilor de informaţii prin analizarea culegerii datelor brute, care, după ce au fost corelate şi analizate, formează baza judecăţilor şi evaluărilor din domeniu. Diversele metode de culegere („disciplinele” domeniului informaţiilor) pot fi clasificate astfel: 1) culegerea din surse

umane (la care se face referire ca spionaj, culegere de informaţii din surse umane sau, în jargonul american, *humini*); 2) culegerea prin metode tehnice (informaţii tehnice sau *ţechini*); 3) culegerea „pe faţă”, prin contacte diplomatice sau din surse accesibile oricui, precum ziarele, site-urile sau alte resurse disponibile pe Internet şi emisiuni de radio şi televiziune (culegerea din surse deschise) 1.

Culegerea informaţiilor din surse umane

Culegerea informaţiilor din surse umane, sau spionajul, reprezintă primul lucru la care se gândeşte cineva când vine vorba de „serviciile de informaţii”. Aceasta implică de obicei identificarea şi recrutarea unui oficial străin care, prin poziţia de încredere pe care o ocupă în guvern, are acces la informaţii valoroase şi care doreşte, din anumite motive, să le transmită ofiţerilor unui serviciu de informaţii. În unele cazuri (în special în timp de război), persoana care furnizează informaţiile poate să nu fie un oficial guvernamental, ci o persoană particulară ce are ocazia să observe (sau să audă despre) aspecte de interes, precum sosirea sau plecarea unor nave dintr-un port. Cel care este recrutat poate fi, de asemenea, o persoană care are acces la informaţii importante în virtutea unei relaţii apropiate (de prietenie, de afaceri etc.) cu cineva de interes pentru domeniul informaţiilor (de exemplu, un terorist sau un traficant internaţional de arme).

În mod obişnuit, sunt implicate persoane cu două roluri diferite: un *ofiţer* de informaţii, angajat al unui serviciu de informaţii, şi o *sursă*,

care îi furnizează ofiţerului date pentru a fi transmise conducerii serviciului de informaţii. Ofiţerul de informaţii sau „intermediarur păstrează legătura cu sursa, transmite instrucţiile primite de la superiori, asigură resursele necesare (precum echipamentele de copiere sau comunicaţii) şi, în general, încearcă să asigure continuitatea fluxului de informaţii2.

Tipuri de ofiţeri de informaţii

Deoarece ofiţerii de informaţii nu trebuie să atragă atenţia guvernului din ţara în care operează, aceştia nu îşi pot declara public intenţia de a oferi bani în schimbul unor date secrete. Aceştia trebuie să aibă ceea ce în jargonul domeniului se numeşte „acoperire” – adică un motiv plauzibil pentru a se afla în acea ţară, metode vizibile de susţinere financiară, un pretext pentru a se întâlni cu persoane care au acces la informaţii de importanţă deosebită şi aşa mai departe3.

În limbajul actual din SUA, se face diferenţa între acoperire „oficială” şi cea „neoficială”. *Acoperirea oficială* se referă la deghizarea unui ofiţer de informaţii în diplomat sau într-un alt tip de funcţionar guvernamental care este trimis în străinătate. Acoperirea neoficială se referă la orice alt tip de deghizare – ca om de afaceri, jurnalist, turist etc. –, ceea ce ar putea justifica prezenţa unui ofiţer în ţara respectivă. Un agent sub acoperire neoficială îşi poate ascunde, de asemenea, naţionalitatea, pretinzând a fi dintr-o altă ţară decât în realitate4. Dacă ţara-gazdă este una care de obicei acceptă imigranţi, ofiţerul

poate intra sub această acoperire.

Folosirea unei acoperiri oficiale are mai multe avantaje. În mod clar, îi poate oferi ofiţerului de informaţii imunitate diplomatică. Dacă activităţile sale de spionaj sunt detectate, legea internaţională delimitează strict condiţiile în care guvernul ţării-gazdă poate să îl declare *persona non grata* şi să îl expulzeze din ţară.

În plus, statutul de diplomat asigură accesul ofiţerului de informaţii la anumite surse; în calitate de diplomat, acesta s-ar putea întâlni, l-ai a a ridica suspiciuni, cu oficiali guvernamentali ai ţării-gazdă în adrul activităţii sale obişnuite, precum şi cu alţi diplomaţi aflaţi la l»ost în aceeaşi capitală. Dacă şi alte ţări vor folosi o acoperire oficială pentru ofiţerii lor de informaţii, va avea ocazii „nevinovate" de a se întâlni cu aceştia a.

De asemenea, trimiterea sub acoperire oficială, la post, a unor aeenţi de informaţii garantează că, în cazul în care un cetăţean al lăiii-gazdă abordează ambasada în legătură cu anumite materiale i onfidenţiale sau o ofertă pentru a le furniza, problema poate fi le/olvată de un profesionist în domeniul informaţiilor. În acest sens, existenta unor ofiţeri de informaţii cu acoperire oficială facilitează încercarea ţării-gazdă de a contacta serviciul de informaţii; astfel de posturi sunt folosite drept „căsuţe poştale" pe cât de utile, pe atât de necesare, în special în ţările ce reglementează strict sau le interzic» eiăţenilor călătoriile sau comunicarea cu lumea exterioară6.

Acoperirea oficială presupune, de asemenea, avantaje administrative. Ofiţerul poate fi plătit şi

se pot rezolva alte probleme legate de personal prin canalele guvernamentale obişnuite, iar comunicaţiile securizate cu serviciul de informaţii pot fi menţinute prin „staţia” de informaţii (grupul de ofiţeri de informaţii sub acoperire oficială) 7.

În acelaşi timp, acoperirea oficială are şi câteva inconveniente. Cel mai important, din cauza numărului relativ redus de oficiali trimişi la post într-o anumită ţară-gazdă, serviciul de informaţii al larii respective poate avea capacitatea de a stabili, destul de precis, i are dintre „diplomaţi” sunt ofiţeri de informaţii şi care nu. Acest lucru se poate realiza prin metode clare, dar laborioase, de menţinere a supravegherii asupra fiecărui oficial şi prin observarea deplasărilor, a contactelor, prin interceptarea telefoanelor, instalarea unor echipamente de interceptare în apartamente şi aşa mai departe. Practica angajării cetăţenilor din ţara-gazdă pentru a lucra în interiorul ambasadelor în anumite posturi facilitează o astfel de supraveghere, în special în acele ţări unde se presupune că orice persoană căreia i se permite să lucreze într-o ambasadă străină a fost de acord să coopereze cu serviciul de informaţii al ţării-gazdă8. În plus, se poate ajunge la acelaşi rezultat prin metode mai simple şi mai puţin costisitoare. De exemplu, materialele publicate de o anumită ţară ar putea fi folosite pentru a urmări cariera ofiţerilor să-i de servicii externe şi a identifica astfel caracteristicile care indică o legătură cu serviciile de informaţii.

Mai mult decât atât, deşi acoperirea oficială

poate asigura accesul facil la potenţialele surse (în primul rând alţi diplomaţi şi oficiali din serviciile secrete ale ţării-gazdă), ea poate obstrucţiona accesul la alte persoane care ar putea ezita să intre în contact cu oficiali străini, în general, sau cu aceia dintr-o anumită ţară. În oricare dintre cazuri, potenţialii recruţi sunt atenţionaţi că intră în contact cu un oficial al unui guvern străin şi astfel devin mai precauţi. În plus, dacă relaţiile diplomatice se deteriorează, cum se poate întâmpla în cazul unei crize puternice sau al unui război – când este vital să se obţină informaţii de calitate –, ofiţerii sub acoperire oficială părăsesc ţara, prin aceasta întrerupându-se activitatea oricărei reţele de surse pe care ar fi putut-o crea9.

Avantajele şi dezavantajele unei acoperiri neoficiale sunt, în cea mai mare parte, opusul celor deja discutate. Pe de o parte, de vreme ce aceştia pretind a avea diverse profesii şi statute sociale, oficialii fără acoperire oficială (NOC) pot avea acces la diferite surse din diverse medii. De asemenea, aceştia pot pretinde că sunt (sau chiar să fie) fie cetăţeni ai ţării unde sunt trimişi, fie ai unei terţe ţări. Ascunderea legăturii cu guvernul pentru care lucrează îi poate ajuta să intre în contact cu potenţialele surse şi să obţină acces la informaţii. Dacă relaţiile diplomatice sunt întrerupte, aceştia pot să rămână şi continue operaţiunea. În general, NOC sunt mai greu de identificat de către guvernul-gazdă.

Pe de altă parte, acoperirea neoficială presupune multe dezavantaje. Cheltuielile şi dificultăţile administrative în asigurarea acoperirii

neoficiale sunt mai mari decât în cazul acoperirii oficiale. Una dintre metode este convingerea unei corporaţii sau a altei organizaţii private să-i permită unui ofiţer de informaţii să fie angajat în cadrul său. O altă soluţie ar fi ca ofiţerii să pună bazele unei afaceri sau să se implice în alte activităţi care să justifice prezenţa lor în ţara-ţintă. Totuşi, această metodă nu numai că presupune cheltuieli majore, ci şi un efort de durată din partea ofiţerului de informaţii pentru a crea o acoperire convingătoare a activităţii sale, ceea ce ar reduce timpul şi efortul pe care ofiţerul le-ar putea dedica activităţii sale principale de culegere a informaţiilor10. Comunicaţiile pot fi mai dificile, din îi ion lent ce NOC nu poate folosi în mod regulat serviciile de comunicaţii *W* ambasadei fără a trezi suspiciuni.

I În bine cunoscut NOC a fost Richard Sorge, un cetăţean german, loicspondent al unui important ziar din Germania, care a spionat pentru serviciul militar de informaţii sovietic în China şi Japonia din unii 30 până în toamna lui 1941, când a fost arestat. Relaţiile sale api opiate cu personalul ambasadei germane din Tokio, inclusiv cu ambasadorul, i-au asigurat accesul la informaţii privind planurile de i A/boi ale Germaniei şi Japoniei. Cu puţin timp înainte să fie arestat, şi în ce a raportat Moscovei informaţii de importanţă capitală referitoare hi faptul că „Estul extrem al Uniunii Sovietice poate fi considerat la adăpost de atacurile japoneze”. Conform raportului lui Sorge, Japonia l îi»iai a se să nu atace Uniunea Sovietică; în schimb, urma să

declanşeze «iac un împotriva Statelor Unite în Sudul şi Estul Pacificului, precum i împotriva coloniilor britanice şi germane din Sud-Estul Asiei. Malin a transferat liniştit sute de mii de trupe din Est la Moscova, unde ui li urmat să stopeze avansarea Germaniei în iarna 1941 – 1942. Privind i«imspectiv, oprirea trupelor Wehrmachtului înainte de a intra în M»scova a reprezentat un moment de cotitură în desfăşurarea războiului".

Un alt exemplu al folosirii cu succes a unei acoperiri neoficiale, ilustrând valoarea capacităţii de mascare a naţionalităţii, este acela al unui agent israelian, Eli Cohen. Evreu de naţionalitate egipteană, (olicn a emigrat în Israel în 1956, la vârsta de 32 de ani, şi s-a oferit i-a voluntar pentru serviciul de informaţii israelian. A fost trimis de agenţia israeliană de informaţii, Mossad, în Argentina în 1961 pentru aşi construi o acoperire ca om de afaceri musulman, sub pseudonimul Kamal Amin Taabet. După ce şi-a stabilit rapid un număr mare de contacte în comunitatea sirienilor expatriaţi din Argentina, Cohen s-a mutat la Damasc la începutul anului 1962. Înarmat cu scrisori de i «comandare furnizate de noii săi prieteni sirieni din Buenos Aires, «oben a reuşit (cu ceva noroc) să pătrundă în cercurile înalte din Siria. De fapt, avea relaţii atât de puternice, încât, la un moment dat, îi fost folosit ca emisar între noul guvern Baath şi un fost preşedinte exilat al Siriei; altă dată, a fost propus pentru un post în Cabinetul guvernului sirian. După ce a raportat timp de trei ani despre problemele tic ordin politic, militar şi diplomatic, Cohen a fost prins de

serviciul de contraspionaj sirian şi executat în mai 196512.

O utilizare ambiţioasă a acoperirii neoficiale implică ofiţerii care pătrund în ţări străine deghizaţi ca imigranţi obişnuiţi. În mod clar, este mai uşor să introduci astfel de ofiţeri într-o ţară care primeşte în mod obişnuit un număr mare de imigranţi şi vizitatori şi care foloseşte metode mai puţin stricte de control al graniţelor, decât într-o ţară care nu primeşte imigranţi şi în general supraveghează strict vizitatorii şi îşi păzeşte cu atenţie graniţele.

Un exemplu interesant care demonstrează cât timp şi efort era dispusă Uniunea Sovietică să acorde operaţiunilor de acest tip este Ludek Zemenel, un cetăţean ceh recrutat de serviciul de informaţii sovietic (Comisia de Securitate a Statului, cunoscută sub numele KGB, de la iniţialele sale în limba rusă) 13. Folosind identitatea unui anume Rudolf Herrmann (adevăratul Rudolf Herrmann era un german care murise în Uniunea Sovietică în timpul celui de-al Doilea Război Mondial), el a trăit în Germania Democrată timp de un an. Apoi, la sfârşitul anului 1957, a plecat împreună cu soţia sa, de origine est-germană (şi ea ofiţer de informaţii sovietic), şi un fiu minor în Germania Federală, unde părea a fi un refugiat est-german obişnuit".

După ce a stat patru ani în Germania de Vest, Herrmann a emigrat în Canada, unde şi-a deschis o mică afacere, realizând filme publicitare şi comerciale. El a îndeplinit o serie de misiuni minore pentru KGB, cum ar fi întocmirea unor

„rapoarte de personalitate” privind politicienii şi jurnaliştii pe care i-a întâlnit prin intermediul afacerii sale şi menţinerea relaţiilor cu un profesor canadian, care era agent KGB. Totuşi, cea mai importantă misiune a sa a fost ascunderea calităţii sale pentru a putea prelua controlul asupra reţelei de surse canadiene de la „rezidentul” legal (şeful bazei KGB de la ambasada sovietică din Ottawa), în cazul unei rupturi în relaţiile diplomatice dintre Canada şi URSS.

După şase ani petrecuţi în Canada, lui Herrmann i s-a cerut să se mute în Statele Unite, unde a îndeplinit misiuni similare. Când fiul său Peter a împlinit vârsta de 17 ani, Herrmann l-a recrutat şi pe acesta pentru a lucra în KGB. Întrucât Peter fusese dus de mic în Germania de Vest şi crescut de la vârsta de 4 ani în Canada şi Statele Unite, trecutul său nu avea motive să provoace suspiciuni; acesta avea să se pregătească pentru o carieră în guvernul american, unde putea opera ca sursă sovietică pe termen lung („cârtiţă”). Se pare că ar fi putut să facă acest lucru dacă FBI nu ar fi obţinut acceptul de cooperare din partea tatălui său, în urma lansării unor ameninţări cu închisoarea la adresa acestuia, a soţiei şi a fiului.

Combinarea agenţilor sub acoperire oficiali şi neoficiali, pe care guvernul îi angajează pentru a executa activităţi de recrutare, depinde tic mai mulţi factori. În general, cei mai importanţi sunt tipul de informaţii căutate şi modalităţile avute la dispoziţie în vederea obţinerii acestora. În cazul Statelor Unite şi al aliaţilor săi, în perioada

Războiului Rece, acţiunea de recrutare de persoane care să acţioneze împotriva Uniunii Sovietice s-a axat în principal pe intenţiile conducerii sovietice, capacităţile militare naţionale şi eforturile depuse de serviciile de informaţii sovietice împotriva Occidentului. Acest aspect, alături de monitorizarea atentă a tuturor cetăţenilor străini de către serviciile sovietice de securitate, însemna că eforturile de recrutare de personal ale Statelor Unite şi ale altor ţări s-au bazat în principal pe ofiţeri de securitate care acţionau sub acoperire oficială.

De asemenea, în ultimii ani, China a folosit în special ofiţeri sub acoperire neoficială pentru a-şi desfăşura programul de recrutare în Statele Unite; aceasta, în ciuda faptului că serviciile de informaţii chineze efectuează, într-adevăr, activităţi obişnuite de recrutare şi culegere a informaţiilor prin utilizarea unor metode sub acoperire, inclusiv a unor companii de faţadă, programe ştiinţifice şi de schimb de experienţă între studenţi, precum şi delegaţii comerciale şi ştiinţifice. I) e asemenea, serviciile de informaţii chineze utilizează agenţi „inactivi” pe termen lung, care emigrează din China şi se stabilesc ca rezidenţi pe o perioadă îndelungată înainte de a desfăşura activităţi secrete în iar de in care au emigrat. Utilizarea excesivă a agenţilor sub acoperire neoficiali decurge din prioritatea pe care guvernul chinez a acordat-o achiziţionării de tehnologie şi informaţii americane avansate, din natura relativ deschisă a pieţelor comerciale americane, din uşurinţa cu care se poate obţine

drept de reşedinţă în Statele Unite şi din existenţa unei comunităţi largi de cetăţeni chinezi în Statele Unite, printre care se pot amesteca emigranţii nou-veniţi15.

Tipuri de surse de informaţii

Aşa cum putem clasifica ofiţerii de securitate ca fiind sub acoperire oficială sau neoficială, se poate face o diferenţiere între mai multe tipuri de surse de informaţii. Una dintre diferenţele de bază este aceea dintre sursele pe care un ofiţer de securitate, după ce pregăteşte terenul, le recrutează în mod activ în serviciul agenţiei de securitate şi *voluntari*, care se oferă din proprie iniţiativă să ajute agenţia de securitate a unei ţări străine, uneori apelând direct la ambasada respectivei ţări.

Sursele recrutate sunt privite de obicei cu mai multă încredere, întrucât ofiţerul de securitate a avut ocazia de a le studia caracterul şi motivaţia înainte de a le recruta”. În plus, sursele ce urmează a fi recrutate vor fi alese în funcţie de gradul lor de acces la informaţii importante. Cu toate acestea, identificarea şi recrutarea surselor presupun un efort laborios şi îndelungat şi nu există garanţii că până şi cel mai atent aleasă şi studiată sursă va răspunde pozitiv la încercările de recrutare sau „agăţare”.

În plus, asupra voluntarilor planează oricum suspiciunea întrucât există întotdeauna posibilitatea ca un presupus voluntar să fi fost în realitate dislocat de serviciul de informaţii al propriei ţări pentru a oferi date false şi înşelătoare, în scopul de a-şi informa ţara cu

privire la metodele de operare ale serviciilor adverse sau pentru a-i întinde o cursă unuia dintre ofiţerii serviciului advers în vederea arestării sau expulzării acestuia. Cu toate acestea, un serviciu de informaţii ce are suspiciuni prea mari în privinţa voluntarilor poate rata ocazia de a obţine informaţii la care ar fi putut avea acces cu uşurinţă. În istoria serviciilor de informaţii există relatări legate de voluntari care au fost iniţial ignoraţi sau refuzaţi, dar care au sfârşit prin a reprezenta surse valoroase pentru acestea.

Un caz faimos de acest gen l-a avut ca protagonist pe Fritz Kolbe, un reprezentant al Ministerului german de Externe, în timpul Războiului Rece. Misiunea lui Kolbe presupunea selectarea informaţiilor trimise zilnic la Berlin prin telegraf de ambasadele germane din întreaga lume. Informaţiile priveau de obicei teme delicate referitoare la probleme strategice, militare şi secrete, precum şi diplomatice. După ce a reuşit să obţină postul de curier oficial ocazional, în august 1943, Kolbe a călătorit în Elveţia, transportând aproximativ 200 de documente sustrase din dosarele Ministerului de Externe de la Berlin. El a abordat iniţial Ambasada britanică de la Berna. Încercând să evite „agenţii provocatori” sau agenţii germani, britanicii nu au dorit să aibă de-a face cu Kolbe. Atunci, el l-a abordat pe Allen Dulles, şeful operaţiunilor secrete americane din Elveţia. Precaut, dar într-o măsură mai mică decât aliaţii britanici, americanii au lucrat cu Kolbe, care, în urma unor călătorii ulterioare la Berna, le-a furnizat peste 1.500 de

documente secrete germane. Kolbe a fost probabil unul dintre cei mai mari spioni din perioada războiului în favoarea Statelor Unite17.

În afară de o clasificare a surselor, mai putem realiza o diferenţiere i motivelor pentru care acestea furnizează informaţii. Sursele pot fi mânate de credinţe ideologice, etnice sau religioase mai puternice decât legăturile lor cu ţările ai căror cetăţeni sunt; este posibil ca acestea să fie deziluzionate de acţiunile sau ideologiile propriilor lari; pot fi lacome; pot fi persoane cărora le lipseşte echilibrul interior şi doresc să aibă parte de aventură; doresc să se răzbune din cauza unui presupus tratament necorespunzător din partea guvernului; sau pot face obiectul unei acţiuni de şantaj. Importanţa relativă a acestor motive depinde de caracteristicile societăţilor implicate şi de tacticile serviciilor de informaţii adverse.

De exemplu, motivaţiile unora dintre americani şi britanici care au ales să îşi trădeze ţara, începând din 1930, nu au mai fost lăcomia şi răzbunarea, ci au avut o natură ideologică. În 1930, sovieticii au aflat că atracţia pe care o exercita comunismul asupra unor studenţi şi asistenţi de la Cambridge University, unii provenind clin familii de seamă, a făcut ca atmosfera ideologică să le fie foarte favorabilă. Printre studenţii recrutaţi la vremea respectivă, care au devenit ulterior importanţi agenţi sovietici infiltraţi în Guvernul britanic, se numără Guy Burgess, Donald MacLean şi Harold („Kim”) l’hilby18.

În schimb, americanii şi britanicii care au fost arestaţi pentru spionaj în favoarea Uniunii Sovietice la sfârşitul anilor ’70 şi 80 par să fi fost motivaţi în special de lăcomie 19. În alt caz, cel al lui Ixlward Lee Howard, fost ofiţer CIA care le-a oferit sovieticilor detalii operaţionale esenţiale privind activităţile agenţiei la Moscova, motivul a fost răzbunarea împotriva CIA, întrucât fusese concediat20.

În general, publicul supraestimează probabil utilizarea sexului pentru a afla anumite secrete şi predominarea şantajului ca motiv pentru activităţi de spionaj, deşi posibilitatea de a recurge la şantaj îi poate permite unui ofiţer să-şi păstreze o sursă care a devenit spion clin alte motive, iar ulterior intenţionează să renunţe. Chiar şi aşa, au ieşit la lumină unele cazuri care presupun folosirea seducţiei şi şantajului, în genul descrierilor din romanele de spionaj.

De exemplu, în perioada celui de-al Doilea Război Mondial, Betty Pack a avut o evoluţie similară cu a celebrei Mata Hari. Căsătorită cu un diplomat britanic, la origine, cetăţean american, Pack a lucrat atât pentru serviciile de informaţii britanice, cât şi pentru cele americane. Strategia ei s-a axat în special pe aventuri cu importanţi oficiali guvernamentali străini. Printre numeroasele sale reuşite, ea a adunat informaţii diplomatice esenţiale de la Ministerul polonez de Externe, înaintea războiului, a obţinut date importante referitoare la eforturile polonezilor de a sparge codurile germanilor, a compromis definitiv acţiunile Ambasadei Franţei ce

reprezenta regimul de la Vichy la Washington şi a obţinut coduri folosite de Marina italiană şi de cea franceză21.

Totuşi, o metodă mai puternică decât seducţia este folosirea sexului pentru a atrage în cursă şi a şantaja un oficial ce are acces la materiale sau informaţii de importanţă deosebită. Un exemplu tipic de acest gen îl are în prim-plan pe Maurice Dejean, ambasadorul francez la Moscova în anii ’50 şi 60. Aflând despre caracterul imoral al ambasadorului căsătorit, KGB a angajat o femeie frumoasă (cetăţean sovietic forţat să coopereze) să-l seducă. După începerea aventurii, cuplul a fost surprins de întoarcerea „neaşteptată” a „soţului” acesteia. „Şocat”, acesta a ameninţat să facă publică povestea şi să-l acţioneze în judecată pe ambasador. Dejean i s-a confesat unui „prieten” rus – în realitate, ofiţerul superior KGB care îi înscenase povestea; „prietenul” s-a oferit să-l ajute pe acesta să păstreze secretul. Planul KGB viza folosirea acestei situaţii compromiţătoare în vederea şantajării lui Dejean, pentru a-l face să lucreze pentru serviciile sovietice atunci când avea să se întoarcă în Franţa, în speranţa că acesta urma să primească o funcţie mai înaltă. Cu toate acestea, planul sovieticilor a fost năruit de defectarea unui scenarist rus, care participase la conceperea intrigii.22

Probleme privind culegerea informaţiilor din surse umane

Multe probleme privind culegerea informaţiilor din surse umane sunt inerente acestei activităţi, în timp ce altele sunt specifice

mai degrabă ţintei serviciilor secrete. În ceea ce priveşte prima categorie, cea mai importantă este asigurarea calităţii controlului – obţinerea certitudinii că informaţiile furnizate de surse sunt corecte.

Din motive financiare, sursele pot fie să fabrice informaţii, fie să în organizeze cu multă imaginaţie sau să înflorească materialele disponibile publicului, pentru a părea că provin din surse extrem de bine plasate (prin folosirea unui jargon al serviciilor de informaţii, crearea unei papermill – fabrică de documente). În istoria serviciilor de informaţii există exemple ocazionale de creatori ai unor asemenea documente prefabricate, care şi-au escrocat clienţii cu sume enorme le bani.

Acest tip de documente prefabricate au proliferat la sfârşitul anilor ’40 şi începutul anilor ’50, exploatând dificultatea serviciilor occidentale de informaţii de a opera în ţările comuniste din Europa de Est. Deseori, acestea erau manipulate de emigranţi săraci din l-ai de respective, care au descoperit la scurt timp că îşi pot câştiga 11.1 lui prin vânzarea unor „informaţii” pe care susţineau că le primesc de la cunoştinţe aflate în poziţii de influenţă în noile guverne comuniste, întrucât aceşti emigranţi erau educaţi şi cunoşteau dedesubturile politice, ei au fost capabili să înflorească şi să interpreteze informaţiile disponibile publicului pentru a produce rapoarte convingătoare23.

O problemă mai gravă privind controlul calităţii decurge din posibilitatea ca un agent să fi

fost „dublat” – ca acesta să lucreze în secret pentru presupusa ţintă şi informaţiile pe care le furnizează presupuşilor să-i angajatori să aibă scopul de a-i înşela. O asemenea dublare poate avea loc în momentul în care o sursă de informaţii este arestată şi alege să coopereze cu cei care au capturat-o pentru a evita diverse pedepse24. De asemenea, sursa ar putea fi un „agent dublu” (o presupusă sursă de informaţii care lucrează în realitate pentru ţara pe care pretinde că o spionează) de la bun început, similar relatărilor de mai sus referitoare la voluntari.

Unele dintre cele mai interesante şi mai remarcabile relatări din istoria serviciilor de informaţii privesc folosirea agenţilor dubli. De exemplu, în timpul celui de-al Doilea Război Mondial, în ceea ce s-a numit „sistemul încrucişat”, britanicii au reuşit să preia controlul şi apoi să manipuleze activităţile germanilor de culegere a informaţiilor din surse umane în Marea Britanie Chiar de la începutul războiului, britanicii au controlat toate rapoartele cu informaţii transmise acasă de presupuşi agenţi germani în Marea Britanie. Printre alte reuşite, aceste rapoarte au ajutat la inducerea în eroare a germanilor cu privire la locaţia şi detaliile privind debarcarea din Normandia. Pe 9 iunie 1944, la trei zile după Ziua Z, un mesaj trimis de o sursă controlată de britanici a avut o importanţă vitală, ducând la blocarea unei divizii germane de tancuri în zona Calais (pentru a împiedica iminenta debarcare a „trupelor principale”, care în realitate nu existau) şi ajutând adevărata forţă de invazie

din Normandia să-şi asigure avanposturile25.

Alte probleme au decurs din natura ţintei. Cu cât este mai eficient şi mai atotpătrunzător sistemul intern de securitate al unei ţări vizate, cu atât apar mai multe dificultăţi în culegerea informaţiilor din surse umane pe teritoriul ţării respective. Un guvern care controlează minuţios călătoriile şi comunicaţiile internaţionale, precum şi alte mişcări, comunicaţii şi activităţi economice ale cetăţenilor să-i în general poate îngreuna extrem de mult desfăşurarea activităţilor neoficiale sub acoperire sau „ilegale" ale unor ofiţeri de informaţii, care intenţionează să călătorească în ţara respectivă, să-şi înceapă activităţile „secrete" şi să opereze fără a fi depistaţi. Ofiţerii care acţionează oficial sub acoperire pot fi ţintele unor acţiuni de supraveghere intensă, ceea ce le îngreunează întâlnirea cu diverşi cetăţeni ai ţării-ţintă fără a fi observaţi. Rezultatul este denumit în jargonul serviciilor de informaţii americane „ţintă dificilă" sau „zonă interzisă", având sensul de o ţară în care activităţile de informaţii se pot desfăşura în general numai sub acoperire oficială şi, chiar şi atunci, cu mare dificultate.

De asemenea, există şi alte ţinte ce ridică probleme specifice. De exemplu, culegerea informaţiilor legate de terorism este limitată de natura relativ restrânsă, secretă şi extrem de omogenă a majorităţii grupărilor teroriste. (Observaţii similare se aplică culegerii informaţiilor din surse umane din rândul reţelelor de crimă organizată.) Deoarece calitatea de

membru al acestor grupări se obţine pe baza prieteniilor, a legăturilor de rudenie sau a activităţilor infracţionale anterioare, devine din ce în ce mai dificilă infiltrarea unui informator în rândul acestora. În acelaşi context, loialitatea existentă într-o asemenea grupare (ca să nu mai vorbim de disciplina pe care grupările le-o impun membrilor lor) îngreunează încercările de a-i convinge pe membri ai acesteia să o trădeze.

Dificultăţile nu se vor sfârşi niciodată, chiar dacă o sursă reuşeşte să se infiltreze într-o grupare teroristă. Pentru a rămâne membru permanent, sursa trebuie să asigure sprijin material pentru acţiuni teroriste sau să participe la acestea. Totuşi, majoritatea agenţiilor de informaţii se simt obligate să stabilească anumite limite în privinţa acţiunilor pe care un ofiţer sau o sursă le poate desfăşura pentru a-şi menţine credibilitatea. În acelaşi timp, utilizarea datelor furnizate de sursă pentru a semnala sau a contracara desfăşurarea unor acţiuni teroriste planificate poate să le indice teroriştilor existenţa unui informator în mijlocul lor şi, în consecinţă, să pună în pericol viaţa sursei. Astfel, este posibil ca agenţia să analizeze îndeaproape planurile interne ale grupărilor de acest gen abia atunci când un membru este capturat.

## Arta schimbului de informaţii

Metodele specifice pe care le foloseşte un ofiţer de informaţii pentru a acţiona şi a comunica cu sursele sale, fără a fi detectat de serviciul de

informaţii advers, sunt cunoscute sub denumirea „artă a schimbului de informaţii”. Cea mai gravă problemă cu care se confruntă un ofiţer de informaţii este posibilitatea ca serviciul advers să-l supravegheze (adică să-l monitorizeze şi să-l urmărească) pentru a-i controla activităţile şi pentru a identifica persoanele cu care acesta intră în contact. Prin urmare, misiunea ofiţerului este de a afla dacă se află sub supraveghere şi, dacă acest lucru se confirmă, de a scăpa de sub supraveghere atât timp cât este necesar pentru a putea intra în contact cu sursele sale sau cu potenţiale surse, fără a risca divulgarea identităţii acestora26.

O tehnică folosită pentru a scăpa de urmăritori, pe care ofiţerii o învaţă la CIA, este ilustrată prin trucul utilizat de Edward Lee Howard – ofiţer eliminat din serviciul CIA – pentru a scăpa de supravegherea FBI în 1985. Într-o seară, pe când se întorcea acasă, iar soţia lui se afla la volan, suspectând că este urmărit de FBI, Howard i-a cerut soţiei să vireze brusc într-o intersecţie întunecoasă; imediat după viraj, acesta a deschis portiera din dreapta şi s-a aruncat afară. În acelaşi timp, soţia lui Howard a umflat o păpuşă în locul lui, făcând să pară de la distanţă că Howard încă se mai afla în maşină. Ea a mers acasă, a intrat în garaj şi a închis uşa acestuia, fără ca echipa de urmărire să îşi dea seama că Howard scăpase şi se putea deplasa în voie27.

În acelaşi fel, până să ajungă la un loc de întâlnire, un ofiţer poate parcurge drumul în câteva ore, creându-şi un adevărat circuit şi

folosind mijloace de transport diferite. Dacă acesta observă că persoana care stă lângă el în metrou a stat lângă el şi în autobuz, poate conchide în mod logic că este urmărit. Echipa de supraveghere poate să nu fie depistată dacă foloseşte un anumit sistem, astfel încât un ofiţer să nu fie urmărit de acelaşi individ pe parcursul unei călătorii. Jocul supravegherii şi al depistării acesteia poate fi nesfârşit de complicat28.

Arta schimbului de informaţii include, de asemenea, tehnici de comunicare cu o sursă, fără a fi necesară o întâlnire. De exemplu, un ofiţer îi poate înmâna discret unei surse un pachet sau un document, în trecere, pe stradă („predare-fulger”). Dacă acest lucru este realizat corect, manevra poate nici să nu fie observată de echipa de supraveghere. Ofiţerul îşi poate pune servieta jos, lângă scaunul său, în timp ce soarbe dintr-o cafea; sursa se aşază la masa vecină şi îşi pune servieta sa, aproape identică celeilalte, jos, lângă cealaltă. Când sursa pleacă, ia servieta ofiţerului, nu pe a sa. Din nou, cu excepţia cazului în care echipa de supraveghere a observat manevrarea servietelor, este posibil ca schimbul să nici nu fie observat.

În acelaşi mod, un ofiţer poate lăsa un bilet într-o locaţie stabilită anterior, cum ar fi în scorbura unui copac dintr-un parc; câteva ore mai târziu, sursa îl recuperează („cutie poştală impersonală”) 29. Dacă ofiţerul plasează biletul fără a fi observat, cel care se află pe urmele sale cu scopul de a afla identitatea surselor va continua pur şi simplu să-l urmărească, fără să realizeze că întâlnirea a avut deja loc. Robert R.

Hanssen, specialist în contrainformaţii al FBI, condamnat recent pentru peste 15 ani de spionaj în favoarea Uniunii Sovietice şi apoi a Federaţiei Ruse, a comunicat în majoritatea cazurilor prin metoda „cutiei poştale impersonale”; evident, cunoscând foarte bine procedurile FBI, acesta a considerat metoda menţionată mai sus drept cea mai sigură30.

O altă măsură de precauţie este evitarea stabilirii întâlnirilor cu o sursă într-o ţară în care aceasta spionează. Este probabil mult mai sigur ca întâlnirea să aibă loc într-o terţă ţară, unde echipele de supraveghere pot fi mai puţin vigilente sau chiar inexistente. De exemplu, Uniunea Sovietică a preferat deseori să stabilească întâlniri i îi surse americane, cum ar fi John Walker (care le-a furnizat sovieticilor numeroase informaţii secrete privind comunicaţiile şi operaţiunile maritime) în Austria, o ţară care, deşi cu un stil democratic incidental, şi-a declarat oficial neutralitatea în timpul Războiului rece.

Cazul Walker a dezvăluit atenţia pe care sovieticii i-o acordă unui agent important. Majoritatea întâlnirilor cu sovieticii au avut loc la Viena, Austria… în timpul acestor întâlniri, Walker şi persoana lui de contact de la KGB obişnuiau să se plimbe pe străzi [,]… [fără a utiliza vreodată] o casă conspirativă în care să se întâlnească, întrucât persoana de contact tocmai venise de la Moscova, iar rezidentura (organizaţia, grup de ofiţeri KGB care lucrau în afara ambasadei sovietice) din Viena nu avea informaţii cu privire

la această operaţiune31.

În alte cazuri, serviciile de informaţii care operează împotriva Statelor Unite au preferat să-şi întâlnească sursele în Canada sau Mexic. Alegerile sunt justificate, având în vedere uşurinţa cu care americanii se pot deplasa în ţările respective şi numărul mare de americani care fac acest lucru. De exemplu, lingvistul şi analistul CIA Larry Wu-tai Chin, mult timp spion în favoarea Republicii Populare Chineze, a efectuat deplasări frecvente la Toronto pentru a primi informaţii de la sursa lui şi pentru a-i înmâna acesteia un film nedevelopat32.

Alte metode clasice privind comunicarea dintre ofiţerii de informaţii Vi sursele lor, fără a fi necesară o întâlnire fizică, presupun „scrieri secrete" şi „micropuncte". Aceste tehnici sunt utile în cazurile în care ofiţerul şi sursa au un motiv aparent nevinovat de a comunica unul cu celălalt, dar bănuiesc că există posibilitatea ca scrisorile lor să fie deschise şi citite de tabăra adversă. Pentru a folosi scrierea secretă, ofiţerul sau sursa va redacta mai întâi o scrisoare aparent inofensivă. Folosind o hârtie de indigo, tratată special, va scrie apoi un mesaj secret deasupra scrisorii originale. Mesajul este invizibil ochiului liber şi devine lizibil numai când hârtia este tratată cu un agent chimic special, cunoscut numai de serviciul de informaţii pentru care lucrează ofiţerul şi sursa. Micropunctele reprezintă o metodă secundară de comunicare; în această situaţie, fotografiile sunt micşorate la dimensiuni microscopice şi ascunse într-un anumit

loc pe hârtie, poate chiar sub o ştampilă sau deasupra semnelor de punctuaţie, în cazul literelor dactilografiate.

## Detectorii

Până acum, discuţiile s-au axat numai pe sursele de informaţii care rămân în funcţie – adică raportează informaţii în timp ce îşi păstrează poziţia oficială ce le permite acces la ele. Aceasta este în mod evident cea mai bună situaţie în cazul culegerii de informaţii, din moment ce presupune păstrarea accesului la ele, precum şi posibilitatea de a „însărcina" sursa cu obţinerea unor documente sau fragmente de informaţii specifice, necesare sau utile. Acest lucru presupune ca orice comunicare dintre o sursă şi agent să rămână secretă, iar sursa riscă să fie prinsă.

Într-o zonă greu accesibilă, aceste dificultăţi se amplifică. În consecinţă, culegerea informaţiilor din surse umane împotriva unor asemenea ţări depinde adesea foarte mult de defectori. Din punctul de vedere al serviciilor de informaţii, acestea constituie surse care nu rămân pe loc, ci mai degrabă fug din ţările de proveniență, de obicei ilegal, şi primesc azil. După al Doilea Război Mondial, culegerea informaţiilor din Occident din surse umane împotriva Uniunii Sovietice a depins în mare măsură de astfel de indivizi. De exemplu, la începutul anilor '50, serviciile occidentale de informaţii nu au avut mare succes în recrutarea unor ofiţeri sovietici de informaţii. Cu toate acestea, în 1954, într-un interval de patru luni,

cinci ofiţeri au defectat în Occident. Aceste defectări au dus la obţinerea unei cantităţi enorme de informaţii privind operaţiunile serviciilor sovietice din primii zece ani după încheierea celui de-al Doilea Război Mondial, în urma defectărilor, s-au aflat importante informaţii secrete privind practicile KGB şi arta desfăşurării operaţiunilor, eforturile organizaţiei de a decripta codurile folosite de alte guverne, infiltrările agenţilor KGB în guvernele occidentale şi implicarea acestora în asasinate33. Similar, Hussein al-Kamal, ginerele dictatorului irakian Saddam Hussein, care a defectat în august 1995, a oferit informaţii valoroase referitoare la programul secret al Irakului privind dezvoltarea unor arme biologice care nu fuseseră descoperite în timpul inspecţiei realizate de Comisia Naţiunile Unite* (UNSCOM) de-a lungul unei perioade de patru ani34.

În ciuda importanţei lor, defectorii pun aceleaşi probleme ca voluntarii. Este greu să fii sigur că aceştia sunt într-adevăr defectori, şi nu cetăţeni loiali trimişi de guvernul ţării lor pentru a dezinforma rivalii. Se impune un oarecare scepticism în relaţia cu aceştia, cel puţin la început. Informaţiile contradictorii furnizate de unii defectori sovietici de seamă în Statele Unite – în special cu privire la prezenţa în absenţa unei „cârtiţe” sovietice plasate într-o poziţie înaltă în guvernul american – nu au fost nici până în prezent pe deplin desluşite; acestea au pus în dificultate serviciul american de informaţii de-a lungul unui sfert de secol35.

## Culegerea informaţiilor din surse tehnice

Culegerea informaţiilor din surse tehnice (sau *techint*, în jargonul serviciilor americane) se referă la un set de metode prin care informaţiile sunt culese folosind mai degrabă tehnologia avansată decât agenţi umani. Limitate în ultimă instanţă numai de ingeniozitatea umană şi de legile fizicii, aceste tehnici presupun fotografierea de la mare distanţă şi interceptarea unor unde electromagnetice, deşi sunt exploatate şi alte mecanisme (de exemplu, semnale acustice).

**Informaţii rezultate din fotografii şi imagistică**

Informaţiile rezultate din fotografii şi imagistică(*photint* sau *imint*), aşa cum relevă denumirea, se referă la fotografierea în vederea i alegerii de informaţii. Mai exact, se realizează fotografii de la «lisianţă pentru a obţine imagini ale unor locaţii sau obiecte la care nu este posibil accesul direct. Această idee a fost pusă în practică sub inima unei supravegheri aeriene, tehnică apărută aproape în acelaşi timp cu inventarea avionului36.

UNSCOM – Comise a ONU creată în 1991, după Războiul din Golf, pentru monitorizarea capacităţilor balistice şi a armelor de distrugere în masă ale Irakului (n.r.).

La începutul Primului Război Mondial, în august 1914, Forţele Aeriene Regale Britanice au realizat supravegherea aeriană a trupelor germane care înaintau pe teritoriul Belgiei37. Odată cu încheierea primei perioade a mişcării,

când germanii şi armatele aliate s-au trezit faţă în faţă de-a lungul unui front ce se întindea din Elveţia până la Marea Nordului, supravegherea aeriană a fost considerată un substitut pentru acţiunile de patrulare ale cavaleriei, care nu mai putea parcurge zona aflată de-a lungul şi în spatele liniilor inamice. Aşa cum scria generalul de brigadă William Mitchell, apostolul american al forţei aeriene din perioada interbelică „un zbor deasupra frontului mi-a oferit o imagine mult mai clară asupra modului în care erau dispuse armatele decât mi-ar fi oferit o patrulare la sol” 38. De aici şi până la amplasarea unor camere de luat vederi pe aceste avioane şi dezvoltarea unei capacităţi aeriene de fotorecunoaştere nu a fost decât un pas.

Odată cu dezvoltarea ulterioară a aviaţiei şi fotografiei, foto-recunoaşterea aeriană a devenit o sursă importantă de informaţii secrete în timpul celui de-al Doilea Război Mondial. Această metodă a fost utilizată nu numai pentru a depista dispunerea şi deplasarea forţelor inamice, ci şi pentru a urmări progresele tehnologice. Prin urmare, britanicii au folosit fotorecunoaşterea aeriană şi alte surse de informaţii pentru a spiona descoperirile tehnice ale germanilor, cum ar fi sistemele radiogoniometrice pe care germanii le-au inventat pentru a-şi ghida bombardierele către ţinte din Anglia, noile radare aeriene de apărare, precum şi rachetele V-1 şi V-239.

Exemplele oferite până acum din domeniul fotorecunoaşterii datează din perioada războiului. Acest lucru nu este întâmplător. În perioada

războiului, interesele armate în vederea realizării unor asemenea activităţi au fost mai mari, iar obstacolele politice prea puţine. Nu numai că este mai important să cunoaştem evenimentele care se petrec în ţara inamică pe timp de război, dar metodele alternative pentru a afla aceste lucruri sunt extrem de puţine. Nu ne putem baza numai pe rapoarte primite de la jurnalişti, călători, diplomaţi sau ataşaţi; în general, relatările din presă sunt controlate îndeaproape, graniţele sunt închise, iar călătoriile în interiorul ţării-ţintă sunt restricţionate, atât pentru cetăţenii ţării, cât şi pentru cei ai altor state neutre. În acelaşi timp, legea internaţională care interzice survolarea teritoriului altei ţări fără consimţământul acesteia nu mai reprezintă un obstacol politic.

Chiar şi aşa, dificultăţile cu care s-au confruntat Statele Unite în încercarea de a desfăşura activităţi de culegere a informaţiilor din imi4 umane împotriva Uniunii Sovietice imediat după sfârşitul celui i «I Doilea Război Mondial le-au făcut să ia în considerare posi-hihiaiea utilizării activităţii de fotorecunoaştere pe timp de pace. v «a interes a fost consolidat atunci când, în 1950, exista temerea

— «m cumva invadarea Coreei de Sud de către Coreea de Nord să îi (h ale un imbold pentru o invazie sovietică în Europa de Vest. i Mn i auza surselor umane insuficiente, Statele Unite s-au temut că h«rai îi de sovieticilor pentru o asemenea invazie s-ar putea să nu fie în laie. În plus, nu prea existau informaţii privind „ordinul de uae „al sovieticilor (dimensiunea şi structura forţelor

armate), lucru în h igreuna extrem de mult eforturile Guvernului american de a-şi – lui.i cheltuielile necesare în domeniul militar.

l hi exemplu de lipsă a datelor concrete privind forţele sovietice i i constituit presupusul „decalaj al bombardierului" la jumătatea nul»i 50. Statele Unite deţineau extrem de puţine informaţii referitoare îi planurile sau capacităţile sovietice de construire a unui bombardier iiirtlegic sau „înarmat" (un avion capabil să transporte o armă Hm leară la distanţe mari între continente). Cu toate acestea, la lemonia de sărbătorire a Zilei Forţelor Aeriene Sovietice, în iulie l» v», imediat înaintea summitului de la Geneva al celor „Patru mari puicii" (Statele Unite, Uniunea Sovietică, Franţa şi Marea Britanie), mi masat al forţelor aeriene americane a văzut survolând 28 de bombar-illerc de mari dimensiuni, un model relativ nou. Se pare că sovieticii în muraseră un program în vederea construirii unor bombardiere îl ni legice care, date fiind planurile de apărare ale Statelor Unite, turnau să creeze o prăpastie în acest domeniu – denumită „decalajul Im inibardierului" – între capacităţile americanilor şi cele ale sovieticilor. Totuşi, ataşatul fusese păcălit de un simplu vicleşug: el nu văzuse de bombardiere noi, ci un număr mai mic care au survolat zona de mai multe ori40. Cu toate acestea, în absenţa unor informaţii i imercte, raportul ataşatului a devenit punctul de pornire în vederea»e în ilarilor de mărire a bugetului american pentru domeniul apărării.

S-au făcut mai multe încercări de a se depăşi

această lipsă de minunaţii privind Armata sovietică. Unul dintre proiecte, denumit Moby Dick”, presupunea lansarea unor baloane în Europa de Vest, pl, lupate cu camere de luat vederi îndreptate spre pământ. Ideea era «a aceste baloane să ajungă apoi în Uniunea Sovietică, purtate de vânturile dinspre Vest, până ajungeau în Japonia sau în Oceanul hie ilic. În acel moment, camerele urmau să fie desprinse printr-un semnal radio şi recuperate. În realitate, multe dintre baloanele respective au aterizat în URSS, permiţându-le sovieticilor să analizeze tehnologia camerelor. În orice caz, din cauza mişcării necontrolate a baloanelor deasupra Uniunii Sovietice, fotografiile developate de pe filmele recuperate au dezvăluit probabil informaţii nesemnificative”.

Pe 21 iulie 1955, la summitul celor „Patru mari puteri”, Preşedintele Dwight D. Eisenhower a propus planul „spaţiilor aeriene deschise”, care viza supravegherea reciprocă a Statelor Unite şi a Uniunii Sovietice. Conform planului, urma ca aceste două ţări „să-şi ofere reciproc un plan complet al obiectivelor militare… dintr-un capăt al ţării până în celălalt”, fiecare urmând să aibă dreptul de a desfăşura activităţi de supraveghere aeriană deasupra teritoriului celeilalte aşa cum considera de cuviinţă42. Eisenhower era de părere că acest plan avea să împiedice orice încercare de a lansa un atac neaşteptat; în opinia sa, un potenţial atacator nu putea spera să iniţieze un atac-surpriză dacă era supus unei supravegheri aeriene permanente. Supravegherea avea, de

asemenea, să faciliteze semnarea unor acorduri ulterioare de dezarmare, deoarece în acest fel sö putea stabili dacă şi cealaltă parte îşi respectă obligaţiile.

Cu toate acestea, Eisenhower nu a dorit să-şi condiţioneze planurile în vederea desfăşurării unor activităţi mai eficiente de culegere a informaţiilor despre sovietici. Opt luni mai târziu, pe 24 noiembrie 1954, el a aprobat în secret construirea unui nou avion care să desfăşoare misiuni de recunoaştere, U-2, ce putea să zboare la aceeaşi înălţime ca şi avioanele de luptă ale sovieticilor şi rachetele sol-aer (SAM). În plus, s-a anticipat că fotorecunoaşterea din sateliţi era o idee fezabilă43. În orice caz, premierul sovietic Nikita Hruşciov a respins propunerea privind „spaţiile aeriene deschise", caracterizând-o drept o încercare de legalizare a spionajului. Pe 21 iunie 1956, Eisenhower a aprobat în secret primul zbor al avionului U-2 deasupra teritoriului sovietic".

De-a lungul următorilor patru ani, zborurile U-2, atât deasupra teritoriului sovietic, cât şi de-a lungul graniţelor sale, au oferit o multitudine de informaţii, furnizând pentru prima dată Statelor Unite o imagine de ansamblu asupra unor importante unităţi şi baze militare sovietice de testare. Sovieticii au protestat pe căi diplomatice împotriva survolărilor, însă, în primă fază, nu au putut să facă nimic în acest sens. Totuşi, a fost doar o problemă de timp până ce sovieticii au elaborat o serie de mijloace capabile să atace avioanele U-2. Pe sime) ni, MAŞINI ŞI BIBLIOTECI: CULEGEREA INFORMAŢIILOR 55

I iun l % O, aceştia au reuşit să doboare unul dintre avioane, capturând pilniul, Francis Gary Powers.

(îi toate acestea, chiar înaintea incidentului în care a fost implicat n Ionul U-2, Statele Unite demaraseră construirea unui satelit cu i i t.itităţi de fotorecunoaştere45. Cu toate că în stadiul de elaborare”» discutat în mod deschis despre construirea acestei staţii, existenţa i i fost, pentru început, considerată strict secretă47. Totul a rămas.«ni până în 1978, când preşedintele Jimmy Carter, dorind să fii lilice nevoia unui al doilea Tratat SALT* (Strategic Arms Limitation hinily) în faţa poporului american, a confirmat public că Statele I linie deţineau o astfel de resursă; existenţa sa fusese un secret timp de in m mulţi ani. Odată cu încheierea Războiului Rece, existenţa şi al»-mintea Biroului Naţional de Recunoaştere (Naţional Reconnaissance l în e NRO) – agenţie cu atribuţii privind „cercetarea şi dezvolluirii, achiziţionarea şi operarea sistemelor de culegere a datelor din paliul cosmic şi din spaţiul aerian” menită „să satisfacă nevoile de înhumare ale Guvernului Statelor Unite” – au fost făcute publice48.

I’senţa activităţilor de fotorecunoaştere o reprezintă calitatea şi puterea echipamentelor optice utilizate pentru captarea şi concen-liniea luminii reflectate de obiecte aflate pe pământ. Alegerea altitudinii la care se deplasează satelitul presupune un compromis Iulie calitatea imaginii (alte aspecte fiind egale, cu cât se deplasează imn jos pe orbită, cu atât va fi mai bună calitatea) şi

intervalul de mnp în care satelitul se poate înălţa (dacă satelitul traversează sferele în m înalţe din atmosfera pământului, rezistenţa acesteia îl va încetini, i va (ace ca greutatea lui să-l atragă spre pământ). Alţi factori care determină deplasarea pe orbită se referă la cerinţe privind optimi/a rea capacităţii de fotografiere a anumitor părţi ale suprafeţei p.imamului şi amplasarea unui satelit în funcţie de poziţia soarelui pentru ca fotografiile să fie făcute în condiţii optime de iluminare. O «lilu uitate aparte întâlnită în fotografierea din spaţiu este că lumina II Hm le să penetreze întreaga atmosferă, ce are tendinţa de a o difuza, iltit and astfel la estomparea imaginii. În schimb, camerele folosite pentru captarea imaginilor din spaţiu, spre deosebire de cele umplasate pe avioane, nu sunt expuse la vibraţiile produse de motorul uimi avion cu reacţie sau la turbulenţele atmosferice49.

SALT (I şi II) se referă la două runde de tratative dintre Uniunea Sovietică şi SUA pe tema dezarmării (n.r.).

La început, toţi sateliţii folosiţi pentru acţiuni de fotorecunoaştere utilizau camere de filmat puternice care, la o comandă efectuată de la sol, evacuau filmul într-o capsulă; capsula era recuperată în timp ce cobora din spaţiu, iar filmul era developat şi analizat. Din anumite motive – cum ar fi deplasarea îndelungată într-o anumită direcţie sau identificarea şi localizarea obiectivelor militare fixe –, timpul scurs între momentul fotografierii, pe de o parte, şi developarea şi analizarea fotografiilor, pe de altă parte, nu a constituit o problemă. Cu toate

acestea, a apărut o dificultate legată de sistemul de recuperare a filmelor – mai exact, legătura cu ţintele mobile sau evenimentele care se desfăşurau rapid. De exemplu, o întârziere de câteva zile ar putea duce la eşecul unui atac-surpriză.

Pentru a accelera procesul, filmul poate fi înlocuit de un dispozitiv cu semiconductori fotosensibili cunoscut sub numele circuit cu cuplaj de sarcină (CCD). Odată ce lumina atinge unul dintre aceşti semiconductori, se produce un semnal electric proporţional cu intensitatea luminii. Măsurând magnitudinea acestor semnale asupra unor elemente individuale ale CCD şi notând cu exactitate unde anume în grilă se află un anumit element, un procesor poate reconstitui din aceste informaţii o imagine fie pe film, fie pe computer. Întrucât există o întârziere infimă de la realizarea lor în spaţiu până când acestea ajung la o staţie aflată la sol, imaginea unei ţinte poate fi reprodusă pe pământ aproape „în timp real” – cu o întârziere nesemnificativă50.

În ciuda acestor îmbunătăţiri, orice capacitate de fotorecunoaştere încă mai depinde de lumina soarelui şi de absenţa umbrei produsă de un nor. Pentru a depăşi aceste limitări, prin folosirea radiolocatoarelor sau a undelor prin infraroşu (emise de obiecte calde sau fierbinţi), se pot folosi alte tipuri de imagini. De exemplu, în loc să se bazeze pe lumina soarelui, reflectată în mod natural de un obiect de pe pământ pentru a produce o imagine, un sistem de recunoaştere cu radiolocator transmite unde radio către zona-ţintă

de jos, receptează undele reflectate de diverse obiecte şi, printr-un proces complex, converteşte datele respective într-o imagine51. Prin „luminarea” ţintelor, independent de soare, şi folosirea lungimilor de undă care pot penetra norii, ceaţa sau precipitaţiile, sistemele de recunoaştere cu radiolocatoare pot asigura, indiferent de condiţiile meteorologice, o capacitate de capturare a imaginilor, pentru o perioadă de 24 de ore.

Similar, o altă componentă a spectrului electromagnetic, undele h îţi ui osii, poate fi utilizată pentru detectarea obiectelor care sunt ni. Îi calde (sau mai reci) decât altele din jurul lor. De exemplu, pe iiinpul zilei, formarea imaginilor prin infraroşu permite desluşirea liun/.işului (care are o „marcă” de căldură) de orice camuflaj (ce are unii diferită). Noaptea, întrucât obiectele încălzite pe timpul zilei au Mimuri diferite de răcire, un sistem cu infraroşu îi poate permite unui analist să detecteze mai multe tipuri de obiecte şi ţinte. De i templu, la apus, obiectele metalice, cum ar fi tancurile, se răcesc mul! mai lent decât terenul sau vegetaţia din jur; această diferenţă poate li surprinsă printr-un sistem de captare a imaginilor prin luliaroşu, facilitând localizarea tancurilor respective la asfinţit52.

O ricât de impresionante şi utile pot fi aceste capacităţi de recunoaştere prin imagini, ele prezintă totuşi un neajuns – calitatea Imaginilor pe care le realizează. În general, rezoluţia (în sens larg, dimensiunea celui mai mic obiect care poate fi detectat) a fotolii al iilor realizate la lumină

naturală este mai bună decât a celor în ah/.ale prin intermediul undelor radiolocatoare sau al altor tipuri dr unde din spectrul electromagnetic. Pentru anumite scopuri, cum h h deplasarea în masă a trupelor, pot fi suficiente imaginile cu ievoluţie scăzută ale unei zone întinse. Cu toate acestea, pentru alte în opuri, cum ar fi constatarea caracteristicilor tehnice ale unui sistem tpccial de arme, se impune o mai mare precizie. Un factor determinant în implementarea eficientă a unor asemenea sisteme de in prindere a imaginilor este cunoaşterea nivelului rezoluţiei necesar pentru a răspunde întrebărilor pe care le-ar putea avea guvernul leleritor la potenţialii săi adversari sau rivali pe câmpul de luptă.

A trecut mult timp de când activităţile de fotorecunoaştere din ipaliu au început să constituie apanajul exclusiv al serviciilor de informaţii americane şi sovietice. Şi alte ţări şi-au lansat sateliţi pentru a face fotografii în scopul obţinerii de informaţii. Odată cu dezvoltarea tehnologiilor relevante, din ce în ce mai multe state pot face acest lucru, dacă doresc şi îşi permit să cheltuiască resursele necesare. Printre ţările care şi-au lansat sateliţi sau intenţionează să facă acest lucru se numără China, Franţa şi Japonia53.

O măsură în acest sens a fost dezvoltarea capacităţilor de fotore-iunoaştere în scopuri comerciale. În 1986, o agenţie guvernamentală din Franţa a lansat un satelit de captare a imaginilor în scop de recunoaştere (Satellite pour l’Observation de la Terre [SPOT]) care a oferit spre vânzare fotografii alb-negru la o rezoluţie pe

zece metri, în 1999, Ikonos, o companie din SUA, a intrat pe piaţă cu o fotografie cu o rezoluţie de un metru; compania intenţiona să ofere fotografii cu o precizie chiar mai mare (o rezoluţie de o jumătate de metru) începând din 2004 şi a obţinut deja permisiunea Guvernului Statelor Unite de a realiza aceste lucruri54. Alte servicii comerciale de recunoaştere sunt oferite sau planificate de companii ori agenţii guvernamentale din Rusia, Africa de Sud, Canada, India, Australia, Israel, China şi Brazilia55.

Culegerea informaţiilor din semnale

Culegerea informaţiilor din semnale (sau *sigint*) reprezintă procesul de extragere a informaţiilor din unde electromagnetice interceptate, denumite în general semnale. În funcţie de tipul de unde electromagnetice interceptate, acest tip de culegere a informaţiilor se poate împărţi în următoarele categorii:

obţinerea unor informaţii prin interceptarea comunicaţiilor cuiva (mesaje radio) de către altcineva decât destinatarul – informaţii obţinute din comunicaţii sau *comini*; interceptarea, procesarea şi analizarea telemetriei străine (semnale radio care le transmit inginerilor informaţii de la senzori aflaţi la bordul unui vehicul de testare despre caracteristicile de zbor sau despre performanţe) – informaţii obţinute din telemetrie sau *telint*; interceptarea, procesarea şi analizarea radiaţiilor electromagnetice care nu sunt emise de un sistem de comunicaţii, ci provin de la un echipament militar (cum ar fi un radar) în timpul funcţionării – informaţii obţinute din surse

electronice sau *elint56*; în principiu, orice undă electromagnetică, emisă fie ca o parte necesară sau ca un derivat al funcţionării unui echipament electric face subiectul interceptării unui receptor corect amplasat şi reglat şi suficient de sensibil57.

Informaţii obţinute din comunicaţii {*comint*)

l în această varietate de informaţii obţinute din semnale, cea mai im he este *comint*, contemporană practic cu utilizarea undelor radio r nit îi comunicaţiile militare şi diplomatice58. Spre sfârşitul celui iii»I I) oilea Război Mondial, *comint* (combinată cu analiza metodelor tir iiipiare – prin spargerea codurilor şi cifrurilor folosite la trans

...11 ca mesajelor importante59) a fost, conform informaţiilor disponibile, m, n importantă decât orice altă sursă de informaţii pentru Marile i tiui i, atât pe timp de pace, cât şi pe timp de război60.

Una dintre primele utilizări ale *comint*, documentată public, ilulează din timpul Primului Război Mondial, atunci când Marina i i îi, uucă a făcut eforturi să afle la timp dacă Germania intenţiona să iventureze în Marea Nordului. În plus, la începutul războiului, Im Hameii au deteriorat cablurile de telegraf submarine ale germanilor im legau Germania de America, Africa şi Spania. În consecinţă, telegramele" diplomatice dintre Germania şi zonele respective trebuiau să fie transmise prin radio, riscând să fie interceptate de tain le britanice de monitorizare61.

În ciuda succeselor timpurii, al Doilea Război Mondial a fost veminentul care a marcat perioada de înflorire a activităţii de niedere a informaţiilor

din comunicaţii de către britanici, precum şi

I«americani. Prin operaţiunile denumite „Ultra” şi „Magic”, comuniuliile germanilor şi japonezilor au fost interceptate şi decodate, iar nu număr enorm de informaţii corecte au fost puse cu operativitate la dispoziţia liderilor politici şi militari din Marea Britanie şi America. În îi mp ce evaluarea adevăratelor proporţii ale impactului asupra.1«laşurării războiului rămâne în continuare o misiune istorică dificilă, *comint* au jucat cu siguranţă un rol inestimabil în înfrângerea Aliaţilor de către puterile Axei62.

Unul dintre cele mai concrete cazuri în care a fost esenţială louiribuţia *comint* a fost victoria Marinei Statelor Unite asupra laponezilor în bătălia de la Midway. Japonia spera să profite de succesul său remarcabil de la Pearl Harbor, din decembrie 1941, punând stăpânire asupra insulei Midway, amplasată strategic, şi, în ai est proces, distrugând ce a mai rămas din forţele navale americane în Oceanul Pacific. Dacă planul japonezilor ar fi avut succes, Hawaii ar fi fost vulnerabilă în faţa invaziei, iar Statele Unite s-ar fi văzut nevoite să încheie un acord de pace în condiţiile impuse de Tōkyō. Pentru japonezi era esenţială o victorie rapidă în Pacific deoarece un război prelungit cu Statele Unite, o forţă cu o populaţie mai numeroasă şi o putere mai mare, ar fi dus la un eventual dezastru.

Fără ştirea japonezilor, criptologii Marinei Statelor Unite din Hawaii au interceptat şi au decodat comunicaţiile criptate ale Marinei japoneze. Prin urmare, forţele americane au aflat

dinainte despre planul de atac al Japoniei asupra insulei Midway63. Pe 4 iunie 1942, înarmat cu aceste informaţii, amiralul Chester Nimitz a organizat o ambuscadă asupra flotei navale japoneze, în Nordul insulei, distrugând patru portavioane inamice şi distrugând aproape în totalitate capacitatea Japoniei de a mai desfăşura operaţiuni de o asemenea amploare în Pacific. Bătălia de la Midway a reprezentat o înfrângere decisivă a japonezilor şi un moment de răscruce al războiului; aceasta a pus capăt oricăror speranţe ale japonezilor de a câştiga rapid războiul, dacă mai sperau la acest lucru64.

Deşi ne-am aştepta ca mesajele radio cele mai importante ale unei ţări să fie criptate pentru a li se proteja confidenţialitatea, unele aspecte ale informaţiilor obţinute prin comunicaţii sunt independente de analiza criptică. Din cauza cheltuielilor ridicate şi gradului ridicat de dificultate, este posibil ca un anumit schimb de mesaje pe unde radio să nu fie criptat; de exemplu, comunicaţiile tactice prin voce, cum ar fi între piloţii avioanelor şi turnurile de control de la sol, sunt deseori emise „în eter”. În alte situaţii, traficul de mesaje nu este codificat deoarece se crede, în mod justificat sau nu, că un adversar nu doreşte sau nu poate să le intercepteze ori (din cauza volumului mare de informaţii) să le proceseze. De exemplu, mesajele comerciale nu sunt de obicei codificate, deşi o parte din acestea ar putea constitui subiecte de interes pentru un potenţial adversar. În sfârşit, nu trebuie să subestimăm virtutea inerţiei: de exemplu, Statele

Unite au reacţionat tardiv după ce s-a descoperit că apelurile telefonice, efectuate la distanţe mari, transmise prin piloni cu microunde, era interceptat de alte ţări din locaţii diplomatice amplasate pe teritoriul lor65.

În plus, printr-o tehnică cunoscută ca „analiza traficului" se pot obţine informaţii utile din fluctuaţii ale volumului şi alte caracteristici externe ale comunicaţiilor radio, chiar şi atunci când conţinutul mesajelor nu poate fi înţeles. De exemplu, dacă între sediul general

»! unei armate şi posturile de comandă din subordinea sa se schimbă im «inişnuit de multe mesaje, un analist poate conchide că urmează să aihn loc o operaţiune importantă". Similar, prin mijloace de „depistare *n* direcţiei" sau „DF" – tehnică folosită pentru stabilirea zonei! igrafice din care provine un semnal radio – se poate localiza nava,", ionul sau postul de comandă care îl transmite.

I) e exemplu, în al Doilea Război Mondial submarinele germane «/; *btKits*) care acţionau în larg îşi foloseau staţiile radio pentru a

„Mimica între ele şi cu înaltul Comandament al Forţelor Navale, aflat în uscat. Utilizarea de către flota germană a tacticii „haitei de lupi" împotriva convoaielor aliate impunea un volum mare de transmisiuni Inlic submarinele germane şi comandamentul lor pentru a coordona ahn în de. Totuşi, acest lucru a făcut submarinele vulnerabile la în lumile de radiogoniometrie realizate de posturile britanice şi uimi icane de interceptare radio şi de navele de război care

escortau lonvoaiele. Deşi nu la fel de valoroase ca decriptarea efectivă a nmunicaţiilor navale germane, operaţiunile de radiogoniometrie ale Aliaţilor au reprezentat un instrument important de culegere a informaţilor în Bătălia Atlanticului. În combinaţie cu spargerea codurilor, an lac ut posibil ca multe dintre convoaiele Aliaţilor să evite „haitele ilr lupi" germane în totalitate şi, în timp, au contribuit la eforturile americanilor şi britanicilor de a urmări şi a scufunda submarinele Heimane67.

Deşi cea mai mare parte a surselor tehnice secrete(*contint*) presupune interceptarea mesajelor radio, pot fi interceptate şi mesajele care sunt transmise prin telegraf. Acest lucru necesită acces fizic la telegraf şi, astfel, are o aplicabilitate generală mai mică decât a» ele surse tehnice secrete care implică trafic radio, deşi, în anumite» a/un, poate fi important. De exemplu, pot fi uşor menţinute dispozitive de interceptare pe liniile telefonice de la ambasada sau «onsulatul unui stat inamic din propria ţară.

Din când în când, se pot accesa clandestin, chiar şi în afara graniţelor propriei ţări, cablurile de telefon sau telegraf pe care le foloseşte un inamic. De exemplu, în oraşele divizate Viena şi Berlin, la începutul şi la mijlocul anilor '50, serviciile de informaţii britanice şi americane au reuşit să instaleze dispozitive de interceptare pe i iiblurile folosite de autorităţile militare sovietice. În Berlin, acest lucru a implicat crearea unui tunel secret complicat dintr-un punct aflat în zona americană a oraşului pe sub linia de demarcaţie a

acestei zone, pentru a intercepta cabluri care se aflau în întregime în interiorul zonei sovietice68.

O tehnică asemănătoare este montarea dispozitivelor de interceptare pe cablurile submarine utilizate de un stat inamic. De exemplu, în anii ’70, scafandrii aflaţi pe un submarin american au fixat un dispozitiv de interceptare, în adâncul Mării Ohotsk, pe un cablu submarin ce lega baza navală sovietică de la Petropavlovsk, din Peninsula Kamceatka, de Vladivostok şi Moscova. Scafandrii au ataşat un dispozitiv care înregistra convorbirile; înregistrările erau ridicate în timpul vizitelor periodice la locul respectiv69.

De asemenea, prin mijloace clandestine, este posibil să fie accesat chiar echipamentul folosit pentru transmiterea sau primirea unor mesaje codificate. De exemplu, un fost ofiţer de informaţii britanic povesteşte cum a reuşit serviciul de informaţii la care a lucrat să compromită comunicaţiile diplomatice egiptene prin plasarea unui dispozitiv electronic de ascultare în imediata apropiere a aparatului de cifrare aflat în Ambasada Egiptului la Londra. Dându-se drept angajaţi ai companiei de telefonie veniţi să efectueze reparaţii, ofiţerii de informaţii britanici au putut să planteze într-un telefon din apropiere un dispozitiv capabil să detecteze clar sunetele care se auzeau când egiptenii configurau setările iniţiale ale aparatului. Cu aceste informaţii, spărgătorii de coduri britanici au putut să copieze setările respective pe propriul aparat, un model larg răspândit, şi decodau pe loc comunicaţiile egiptene cifrate. Operaţiuni asemănătoare au

necesitat instalarea unor dispozitive de supraveghere pe maşinile de scris electrice în timpul transportării lor la ambasada unei ţări70.

Progresele tehnologice din domeniul telecomunicaţiilor au ridicat noi probleme activităţii de culegere a informaţiilor prin interceptarea comunicaţiilor. În timp ce interceptarea transmisiunilor radio tradiţionale depinde de capacitatea de a plasa o antenă de recepţie cu o sensibilitate rezonabilă în locaţia potrivită, iar interceptarea liniilor telefonice standard este o chestiune de obţinere a accesului fizic, interceptarea în cazul metodelor de comunicaţie mai noi ridică probleme mai mari. De exemplu, cablurile din fibră optică, adoptate pe scară largă întrucât asigură o lăţime de bandă mai mare (adică posibilitatea de a transmite mai multe informaţii pe unitate de timp)

…de asemenea, mai greu de interceptat decât cablurile pe care le mese71. În mod asemănător, telefoanele celulare, înciuda faptului i uaiisinit pe unde radio, ridică probleme mari din cauza algorit-imilmi complecşi în funcţie de care sunt gestionate apelurile indiviki ui timp ce apelantul se deplasează dintr-o locaţie în alta72.

Ai hvitatea de culegere a informaţiilor imn mijloace telemetrice {*telint*)

Halle forme de *sigint* sunt mai noi decât *comint*, reflectând aih/.uca tot mai largă în domeniul militar a fenomenelor electro-Mi.ipiciice. Activitatea de culegere a informaţiilor prin mijloace N Iniicirice sau *telint* este asemănătoare cu *comint*, cu excepţia i tpmliii că respectivele

comunicaţii care sunt interceptate au loc iulie un vehicul-test (ca, de exemplu o rachetă) şi o staţie aflată la sol, şi nu constau în cuvinte, ci în indicaţiile primite de la diverşi senzori,«ilic echipamente aflate la bord. (Aceste comunicaţii sunt cunoscute – li numele de telemetrie – „măsurare de la distanţă”.) Valorile mim în variabile ca acceleraţia vehiculului, temperatura în diverse piiiM ic din interiorul vehiculului, consumul de carburanţi şi aşa mai! p.iiic, luate împreună, îi ajută pe inginerii aflaţi la sol să-şi facă o Mire despre ce se întâmplă în vehiculul-test. Acest lucru îi ajută pe uif meri să remedieze orice probleme care pot apărea în timpul h Mulul şi să îmbunătăţească performanţa vehiculului.

În acelaşi timp, este evident că astfel de informaţii sunt valoroase mâni îi potenţialii adversari. Dacă pot să intercepteze şi să interpieuve aceste fluxuri de date, vor obţine informaţii despre sisteme nu de armament când acestea sunt încă în stadiul de test. (Analiza dalelor de telemetrie este o sarcină foarte dificilă; împreună cu

«ipi, ui, iliza, este discutată în următorul capitol ca un tip de analiză i mloimaţiilor secrete.) Astfel, la fel ca în cazul *comint*, ţara care hiiuează testul poate încerca să le refuze altora accesul la milmimaţiile telemetrice, retransmiţându-le către staţiile de la sol în Nunţii criptată. O altă posibilitate este ca datele de telemetrie să fie incejsirate şi păstrate la bordul vehiculului-test, urmând a fi recul ni ale şi extrase ulterior. Acest proces, numit „încapsulare”, protejează dalele

împotriva interceptării; totuşi, poate fi o procedură riscantă, mti Mcât, în cazul unei defecţiuni catastrofale a vehiculului-test, exact când datele de telemetrie ar fi foarte utile, „capsula" care le conţine poate fi distrusă sau greu de localizat.

Activitatea de culegere a informaţiilor prin mijloace electronice {*elint*)

Activitatea de culegere a informaţiilor prin mijloace electronice, sau *elint*, presupune monitorizarea şi analizarea radiaţiilor electromagnetice utilizate în alt scop decât transmiterea unor mesaje şi care sunt emise de echipamentele militare străine. La bază, *elint* îi permite unei ţări să urmărească elementele-cheie ale forţelor armate aparţinând altei ţări (ca radarele sale antiaeriene, centrele de comandă şi control etc.), asigurând ceea ce este numit uneori o „ordine electronică a conflictului". Sistemul EORSAT (Elint Ocean Reconnaisance Satellite – satelit de recunoaştere maritim pentru culegerea informaţiilor prin mijloace electronice), utilizat de fosta Uniune Sovietică, iar acum de Rusia, este un exemplu de astfel de monitorizare. Ani la rând, aceste dispozitive au fost folosite pentru a localiza şi a urmări navele de război americane prin interceptarea semnalelor electronice de rutină (ca, de exemplu, cele radar) emise de nave din largul mării73.

Cu toate acestea, activitatea de culegere a informaţiilor prin mijloace electronice nu presupune doar detectarea prezenţei unui emiţător. De exemplu, prin interceptarea unui

semnal-radar, se pot determina diverse caracteristici de funcţionare a radarului, ca, de exemplu, raza de acţiune (ce suprafaţă poate scana dintr-odată) şi aria sa maximă de acoperire. De exemplu, aria de acoperire a unui radar ce emite impulsuri individuale poate fi determinată din ritmul cu care se repetă impulsurile (numărul de impulsuri individuale sau „pachete" de unde radio emise pe secundă). Astfel, în timpul celui de-al Doilea Război Mondial, serviciile secrete britanice au dedus, din faptul că radarul antiaerian german Freya funcţiona cu un ritm de repetare a impulsurilor de cinci sute de impulsuri pe secundă, că raza sa maximă de acţiune este de trei sute de kilometri74.

Un caz mai recent ce ilustrează valoarea pe care o are *elint* a avut loc în timpul ofensivei din 1982 a Israelului în Liban. În timp ce Armata israeliană se deplasa pentru a elimina forţele Organizaţiei de Eliberare a Palestinei (PLO) cu baza în Liban, un posibil atac din partea trupelor şi tancurilor siriene concentrate în Valea Bekaa din

I Mul i hanului preocupa înaltul Comandament israelian. Protejarea + Im forţe era un atribut al artileriei SAM siriene. Folosind aparate di /inh mici, fără pilot, cu viteză mică, israelienii au păcălit artileria MUMIA, determinând-o să îşi deschidă radarele de reglare a focului „i. M.iNve aparatele de zbor emiteau semnalele unor avioane obişiiir, apoi, semnalele emise de forţele siriene erau înregistrate de in al doilea set de aparate de zbor israeliene. Pe baza

acestor mii uniaţi i, israelienii au determinat caracteristicile operaţionale ale Milaicloi SAM şi le-au localizat. Drept urmare, în câteva ore, forţele h ne israeliene au distrus aproape toată artileria siriană, au câştigat nilului incontestabil asupra spaţiului aerian al Libanului şi au, hiiimai orice posibilitate reală ca forţele siriene să intre în luptă de paiira l'L075.

Ai hvitatea de culegere a informaţiilor pun măsurători şi semnături (*mas*/ *nf*)

hmitilităţile privind culegerea informaţiilor din surse tehnice sunt iiniiiaie doar de legile fizicii şi ingeniozităţii umane. Pe lângă photini h ifjffjff, au mai fost folosite şi alte tehnici pentru a culege informaţii. Ai i sica au fost grupate sub denumirea culegere a informaţiilor prin HtJUtirători şi semnături sau *masint*, deşi nu au prea multe în comun nule cu altele (în afară de faptul că nu sunt nici *photini*, nici i»e exemplu, s-au creat senzori speciali care să detecteze şi să îi în uni ice caracteristicile detonărilor nucleare. Printre acestea se miiiaia: seismometrele, care măsoară undele de şoc asociate cu în\icle nucleare subterane; dispozitivele pentru detectarea radioactivităţii asociate cu materiale nucleare sau căderile de pulberi lailmactive din testele nucleare realizate la suprafaţă; senzorii pentru în tarea de la distanţă a fasciculelor de lumină produse de testele în h leare realizate la suprafaţă77. Un alt tip de senzor, sonarul, udi/ază alt fenomen natural, undele sonore, pentru a detecta iilmiarinele aflate în misiune. În afară de locaţia submarinului, pot

Îl determinate şi alte caracteristici ale acestuia în urma unei analize a Mineielor pe care le emite sau le reflectă78.

Platforme pentru culegerea informaţiilor în dezbaterile publice şi în studiul nostru, s-a pus accentul pe culegerea informaţiilor prin sisteme bazate pe sateliţi. În mod evident, sateliţii au avantajul de a survola orice zonă a lumii, fără a ţine cont de graniţele internaţionale79. Din acest motiv, sunt extrem de valoroase pentru culegerea informaţiilor din ţări în care accesul nu este posibil din cauza izolării lor şi a măsurilor stricte de securitate. Cu toate acestea, au şi anumite dezavantaje:

sunt, în general, mai scumpe decât alte platforme de recunoaştere80.

nu se pot apropia foarte mult de ţintele lor (în general, sateliţii aflaţi mai jos pe orbita Pământului rămân la altitudini cu mult peste o sută de mile, pe când cei de pe orbita geostaţionară trebuie să se situeze la o altitudine de 22.400 de mile*); sunt relativ inutili o mare parte din timp, chiar dacă orbitele lor sunt calculate pentru a maximiza informaţiile pe care le culeg (cu alte cuvinte, un satelit de recunoaştere fotografică ce, prin fotografiile pe care le face în Rusia sau Orientul Mijlociu, justifică investiţia realizată, trebuie totuşi, conform legilor fizicii orbitale, să petreacă perioade îndelungate în Emisfera Sudică într-un mod mai puţin eficient); orbitele lor sunt previzibile, deci inamicul poate să îşi avertizeze trupele şi echipamentele sensibile cu privire la momentul în care vor fi vulnerabile la

sateliţii de recunoaştere81.

Astfel, deşi activitatea de recunoaştere spaţială prezintă numeroase avantaje importante, există şi alte tipuri de platforme care continuă să joace roluri semnificative în sfera exploatării tehnice. Avioanele, de exemplu, pot efectua misiuni la periferia teritoriului unui adversar; pot intercepta comunicaţii imposibil de interceptat din spaţiu; pot fotografia zone aflate în apropierea graniţelor teritoriale, rămânând în acelaşi timp în siguranţă în afara spaţiului aerian al ţării-ţintă; şi pot intercepta semnalele radar provenite de la radarele antiaeriene ale adversarului, ce ar fi activate tocmai în scopul identificării traiectoriei avionului. Aparatele de zbor fără pilot (vehicule aeriene fără echipaj sau UAV) pot fi utilizate în zone în

* 1 milă = 1, 609344 km (n.r.).

Mi mijloacele de apărare antiaeriene inamice prezintă un risc

«urm de mare pentru piloţi şi echipajele vehiculelor. Aparatele de Um.hi multe avantaje (care corespund dezavantajelor prezentate în i/mI sateliţilor): sunt mai ieftine decât sateliţii, se pot apropia mai mmli de lintele lor, pot plana deasupra zonelor de interes şi, probabil

I m.îi important, traiectoriile lor nu pot fi anticipate.

Im Războiul din Golf din 1990 – 1991, avioanele de supraveghere \\VAI \S (*Airborne Warning and Control System* – sistem aeropurtat i. ivmizare şi control) şi J-STARS(*Joint Surveillance Target Attack iuliii System* – sistem radar de

supraveghere comună pentru atacarea miM Im) care zburau în spatele liniilor americane le-au permis

Mi.iiRlanţilor americani să urmărească şi să ţintească mişcările de iimhsi aparate de zbor irakiene aproape în timp real. În special i MARS a oferit date critice despre dispunerea forţelor terestre kftkème cu puţin timp înainte de începerea ofensivei declanşate de ilitic, reasigurând coaliţia că manevra sa surpriză din jurul M.mm ului drept al inamicului nu va întâmpina, practic, niciun fel de

IMcntfl. În timpul Bătăliei de la Al-Khafji, în data de 29 ianuarie

I STARS a detectat un convoi irakian de forţe de urmărire care în ilrplasau înspre Sud din oraşul Kuweit. Aceste informaţii le-au 11” n.insmise imediat comandanţilor Coaliţiei, care au ordonat i.u mi i aeriene împotriva trupelor irakiene ce înaintau. În câteva ore, hm Inşi distruse 58 din cele 61 de vehicule ale convoiului82.

I.i ope raţiunea NATO din Kosovo din 1999 (Operaţiunea Forţa MUIA) s-a înregistrat o utilizare „fără precedent” de UAV în scop de in Miioaşlere, „reducându-se necesitatea de a trimite aparate de zbor în lupaj în spaţiul aerian ostil” 83. Flexibilitatea UAV a fost reliefată Im uimitoarea observaţie făcută de înalţii oficiali ai Statelor Unite:

I» *, i s-au pierdut un număr semnificativ de UIW, capacitatea lor de in deplasa deasupra unui teritoriu ostil le-a permis să ofere informaţii im.h iivitatea de supraveghere care nu puteau fi

obţinute prin alte mmli», un şi a eliminat riscul de a pierde echipaje. Mai mult, în! mi i urca UAV s-a urmărit o singură utilizare a acestora, costul milms fund prioritar faţă de durata de viaţă a aparatului”.

IV lângă aparatele de zbor, şi alte platforme pot fi utile pentru

Ith pica informaţiilor din surse tehnice. Furgonetele şi camioanele îmi monitoriza în mod clandestin comunicaţiile şi semnalele echipaţir Mirlor militare, diplomatice sau ştiinţifice în timp ce stau parcatelpiopiere. În mod asemănător, navele pot intercepta semnalele radio de pe coasta unui inamic. Radarele maritime sau terestre, dacă sunt amplasate suficient de aproape de o locaţie de unde se lansează proiectile-test sau unde focoasele reintră în atmosfera Pământului, pot să urmărească testele de zbor cu proiectile ale unui inamic şi să determine unele dintre caracteristicile rachetei. Locaţiile aflate la sol, în funcţie de amplasare, pot, de asemenea, să fie utilizate pentru a intercepta diverse semnale radio, inclusiv semnale care este posibil să fi ricoşat accidental de pe suprafaţa Lunii84. În sfârşit, reducerea dimensiunilor dispozitivelor de ascultare şi ale altor senzori le permite serviciilor de informaţii să culeagă informaţii din surse tehnice atunci când un agent poate să se apropie suficient de ţintă şi să „planteze” senzorul pe ascuns85.

Pe scurt, caracterul platformelor pentru culegerea informaţiilor poate varia de la obişnuit la exotic. Pentru o comunitate de informaţii modernă, avansată din punct de vedere

tehnologic, decizia alegerii unei platforme şi combinaţiile acestora reprezintă, în primul rând, rezultatul a două evaluări: Ce platforme pot culege cel mai bine informaţiile dorite? Care sunt costurile şi riscurile aferente pe care le implică utilizarea anumitor platforme?

Comparaţie între *humint* şi *techint*

De-a lungul anilor, a existat o dezbatere continuă în Statele Unite cu privire la importanţa pe care o au *humint* şi *techint*. Pe de o parte, sunt cei care consideră culegerea informaţiilor din surse tehnice primordială, existând probabilitatea de a continua să îşi sporească însemnătatea rolului pe măsură ce tehnologia progresează. Pe de altă parte, sunt cei care cred că importanţa culegerii informaţiilor din surse tehnice a fost exagerată, în detrimentul spionajului tradiţional, şi că trebuie restabilit acest echilibru.

O contribuţie remarcabilă la această dezbatere a fost apărarea îndrăzneaţă a întâietăţii *techint* prezentată în memoriile amiralului Stansfield 1\irner, directorul CIA din timpul mandatului preşedintelui Carter:

Acum, când avem sisteme tehnice care variază de la sateliţi ce călătoresc în spaţiu deasupra întregului Glob până la aparate de zbor ce ajung în

Mp«il aerian internaţional şi senzori în miniatură amplasaţi pe ascuns Im qnopicrea unor ţinte dificile, nu suntem departe de momentul în care *«ti supraveghea aproape orice punct de pe suprafaţa pământului cu un m/i»i jji, probabil, nu doar cu unul singur. Putem să facem fotografii li

lalute de la distanţe foarte mari, să detectăm sursele de căldură prin luh»/nive cu infraroşu, să localizăm cu exactitate metalul cu detectoare MMgitetice, să facem diferenţa între obiecte care abia se mişcă şi unele imobile eu ajutorul radarelor Doppler, să folosim radarul pentru a şi în îi obiecte care sunt acoperite sau ascunse în întuneric, să interi»i.lui prin toate mijloacele semnale de la vocea umană la unde radio i în ironice, să detectăm radiaţia nucleară cu contoare Geiger exacte şi a iiuegistrăm explozii subterane la distanţe mari cu ajutorul dis în/nivelor seismice. Majoritatea activităţilor pe care intenţionăm să le monitorizăm implică emiterea unor semnale diferite. În conflict, m. mile pot fi detectate după căldura ce provine de la motoare, după magnetismul blindajului sau prin fotografiere. O fabrică de arme… Icare emite radiaţii, are o formă fizică exterioară aparte şi este.i li Mim tată cu anumite tipuri de materiale. Într-un fel sau altul, ar trebui i în curând să putem urmări majoritatea activităţilor de pe suprafaţa i.iMiantului, zi şi noapte, pe vreme bună sau rea86.

I tirajul tehnologic absolut implicat în crearea acestor tipuri de ilUNI/iiive pentru culegerea informaţiilor din surse tehnice este, îi adevăr, extraordinar. Cu toate acestea, admiraţia faţă de teh-mhlmic conduce uşor la o supraestimare a ceea ce poate realiza»n *tuni* şi la o subestimare concomitentă a activităţii de culegere a minunăţiilor din surse umane (*humint*). În Statele Unite, această m*!«icctivă a fost predominantă în special la mijlocul şi la sfârşitul Miilm 70; cu toate

acestea, de atunci, importanţa *humint* a primit îi mutai recunoaştere.

Avaniajele *techint* sunt descrise foarte bine în pasajul citat mai mz Activitatea de culegere a informaţiilor din surse tehnice a fost iMihsieivsabilă în Statele Unite în cazul majorităţii datelor pe care li a obţinut despre Uniunea Sovietică. Cu toate acestea, trebuie M nutreai că, în multe alte ţări, o mare parte a acestor informaţii sunt disponibile în mod public. Informaţii despre mărimea şi structura jrirraH a forţelor armate şi despre dezvoltarea unor importante» în h ic de armament noi, de exemplu, sunt disponibile în majoritatea (tiiloi în documente oficiale (în special bugetare şi parlamentare), i în mare acestea, au fost necesare metode complexe şi costisitoare de exploatare tehnică pentru a culege aceste informaţii despre Uniunea Sovietică, din cauza caracterului secret pe care regimul îl conferi aspectelor militare în special şi celor ce ţin de securitatea naţională în general. O mare parte din activitatea de culegere a informaţiilor din surse tehnice, care s-a realizat de-a lungul anilor, a vizat contracararea efectelor acestui caracter secret.

Cu toate acestea, de la prăbuşirea Uniunii Sovietice şi dizolvarea Pactului de la Varşovia, numărul „ţintelor dificile” s-a redus substanţial şi, odată cu acesta, şi necesitatea de a acorda o pondere atât de mare culegerii de informaţii din surse tehnice. Bineînţeles, încă exist! societăţi închise, iar unele dintre ele, cum ar fi Coreea de Nord, prezintă un interes major pentru activitatea

de culegere a informaţiilor; în acest caz, probabil că va continua tendinţa de a acordi o importanţă mare *techint*. Un caz mai interesant ar fi cel al Republicii Populare Chineze, care rămâne o ţară în care spionajul se realizeazi cu dificultate, dar care este mult mai deschisă în ceea ce priveştd libera circulaţie şi comunicaţiile decât a fost vreodată Uniunea Sovietică.

Mai mult, în ceea ce priveşte o mare parte din categoriile de informaţii pe care toate ţările le ţin secrete – cum ar fi intenţiile şi planurile politice şi militare –, culegerea informaţiilor din surse umane a fost întotdeauna şi încă este necesară. Susţinătorii *humint* subliniază că, în ciuda progresului tehnologic, spionajul tradiţional este în continuare necesar pentru a furniza informaţii despre inteneţiile, activitatea politică şi conceptele strategice ale conducerii unei ţări inamice. Culegerea informaţiilor din surse tehnice, de exemplu, a demonstrat clar comasarea armatei irakiene la graniţa kuweitiană în iulie 1990; ceea ce nu a putut elucida a fost intenţia lui Saddam Hussein: voia să invadeze Kuweitul sau să impună adoptarea unor concesii financiare? în schimb, un agent bine plasat din statul-major al Armatei poloneze a informat cu privire la decizia secretă a Guvernului polonez din 1981 de a impune legea marţială pentru a zdrobi Solidaritatea, mişcarea sindicală independentă87. Pe scurt, înţelegerea intenţiilor inamicului, a strategiei sale şi a percepţiei pe care o are cu privire la situaţia în care se află este, deseori, cea mai de preţ informaţie.

Interceptarea comunicaţiilor dintre conducerea politică şi cea militară a ţării inamice (*comint* la nivel înalt) poate oferi, de asemenea, i*Minţii de acest tip; este ca şi cum ai avea un agent cu acces lui la liderii inamici. Totuşi, obţinerea acestor informaţii prin»*m* este mult mai dificilă decât lasă să se vadă expunerea lui în „i în primul rând, se poate presupune că un adversar îşi., a. n/J majoritatea comunicaţiilor sensibile. În această ordine de

Itchuie remarcat faptul că activitatea de culegere a informaţiilor *Mh* mii xe umane poate fi utilă şi chiar critică şi în această privinţă:

I a. afari liste de coduri sau alte date care facilitează decriptarea m. MMlor. De exemplu, la începutul anilor ’30, serviciile de *inform* «m franceze au obţinut de la un agent din Germania date importante i» que aparatul de codare german numit „Enigma”, inclusiv instruc… i ife utilizare a sa, unele detalii despre construirea lui şi „cheile”.

11 nnxificau modul în care trebuia configurat zilnic aparatul. \. suinformaţii au fost împărtăşite serviciului de informaţii polonez, a făcut progrese criptanalitice majore, ce au stat la baza succesu-l H M» ale l-a avut operaţiunea Ultra a Marii Britanii în timpul celui i… il I hulea Război Mondial88.

În al doilea rând, majoritatea mijloacelor *comint* pot fi combătute

…«iuţind mesajele nu pe calea aerului, ci prin cablu. Interceptarea iMMiiKaţiilor prin „mijloace fixe” necesită obţinerea accesului la i «titlul, ceea ce este un lucru dificil în majoritatea cazurilor.

Mai... li după cum am menţionat deja, cablurile tradiţionale sunt înlocuite

11 aliluri din fibră optică, ce utilizează lumina coerentă (raze laser)

I... îi a transmite mesajele şi sunt mult mai puţin vulnerabile la

HIN heplare.

Im plus, toate tipurile de mijloace tehnologice de culegere a i...Nţiilor, inclusiv *comint*, suferă de un posibil „impediment al

«mit»i ” Având în vedere răspândirea globală a sistemelor de culegere miioi mnţiilor din surse tehnice, trebuie să existe o metodă prin care i h re comande ce ţinte să supravegheze şi pe care să le ignore89.

I i Hiaie fi adevărat că „[în curând] vom putea supraveghea aproape iie i punct de pe suprafaţa pământului cu un senzor”, nimeni nu ar i... i s-a le supravegheze pe toate în acelaşi timp şi, chiar dacă ar

...i. i-ar fi imposibil să proceseze şi să analizeze toate datele pe

Ic ar culege senzorii.

Valcl, existenţa posibilităţilor tehnice, precum cele descrise de limier, înseamnă că aspecte importante la nivel mondial pot trece... i».mate de un serviciu de informaţii bine echipat. După cum a devenit evident în urma inspecţiilor întreprinse după Războiul din Golf, culegerea informaţiilor din surse tehnice de către americani înainte de război nu a fost suficientă pentru a urmări demersurile Irakului de a construi o armă nucleară90. Nu se pune problema daci activitatea de culegere a

informaţiilor din surse tehnice este valoroasa* Pur şi simplu, pământul este un loc cuprinzător, variat şi, în unele zone, foarte activ. În consecinţă, multe depind de capacitatea de g amplasa senzorii în mod corespunzător. Culegerea informaţiilor din surse umane poate oferi primul indiciu esenţial că într-o locaţie dali se întâmplă sau se va întâmpla ceva de interes. Acest lucru face posibilă vizarea zonei respective de către sistemele tehnice. În lipsa acestor indicii, sistemele ar fi mai puţin eficiente şi ar putea rata evenimente importante fie pe perioade lungi, fie în totalitate.

O sursă umană de informaţii poate oferi şi indiciile necesară pentru interpretarea datelor brute strânse de un sistem de culegere a informaţiilor din surse tehnice. Chiar şi cu o fotografie clară a unei clădiri, de exemplu, este posibil ca un expert dintr-un serviciu de informaţii să nu poată identifica ce tip de activităţi se desfăşoară în acea locaţie. Cu toate acestea, o sursă umană cunoscătoare poate să explice că prezenţa unui anumit detaliu, care altfel nu se remar că, indică faptul că respectiva clădire a fost proiectată cu un anumit scop, legat de un anumit program militar. Fără sursa umană, este posibil ca detaliul să nu fie observat sau semnificaţia să nu fie înţeleasă. Dar, odată ce această „semnătură” este recunoscută, pot fi examinate fotografii ale unor clădiri asemănătoare pentru a vedea dacă e prezent acelaşi detaliu.

Totuşi, în mai multe cazuri, semnăturile posibilelor ţinte ale culegerii de informaţii sunt din ce în ce mai greu de identificat sau, dacă sunt

identificabile, sunt greu de urmărit. Uneori, acest lucru se întâmplă deoarece ţintele au devenit mai mici, mai mobile sau subterane. Alteori, cauza o reprezintă faptul că activitatea care interesează serviciile de informaţii (cum ar fi cercetarea în domeniul armelor biologice sau chimice) nu se poate distinge rapid de activităţile conexe, dar legale (ca, de exemplu, fabricarea unor produse farmaceutice sau pesticide). În plus, în unele cazuri poate fi posibil să se elimine în totalitate semnăturile cheie care oferă indicii. După Războiul din Golf, de exemplu, echipa ONU trimisă în Irak pentru a găsi şi a distruge fabricile de arme nucleare din această ţară a

I i. M-i h că Irakul construise cu minuţiozitate multe dintre clădirile în inogram pentru a evita detectarea cu ajutorul sateliţilor şi al altor iii» me Ichnice de culegere a informaţiilor. Unele fuseseră construite i» nu u.1 împiedica emisiile radioactive, în timp ce altele fuseseră i... mic pentru a atrage cât mai puţin atenţia asupra lor, imitând opuiul fabricilor de produse industriale legale. Se pare că abia, lup.i te un inginer irakian care cunoştea încercarea lui Saddam l Im v.nii de a construi o bombă a trecut după război de partea adversă îmi identificate aceste locaţii ca făcând parte din programul buhului de dezvoltare a armelor nucleare91.

Ilttuşi, în ceea ce priveşte unele tipuri de informaţii secrete, H ol»Irma legată de identificarea corectă a ţintelor de către sistemele în Imime de culegere a informaţiilor poate fi aproape imposibil de in /olv. II De exemplu, este

posibil ca *humint* să fie necesar pentru am îi *yv* informaţii cruciale despre ţinte nonguvernamentale (cum ar fi

Mi. Mii/aţiile teroriste) care nu au locaţii stabile sau reţele de… niiicaţii ce pot fi exploatate din punct de vedere tehnic. Altfel hm, cu cât o grupare poate fi asociată cu mai puţine locaţii cunoscute, îi.h.îi este mai greu de vizat de către senzorii tehnici. Culegerea (Mloimaţiilor despre astfel de grupări poate depinde foarte mult de ip.u Halea de infiltrare în ele sau de recrutare a membrilor lor ca mloi maiori. Dacă grupările de acest tip devin ţinte importante ale miviciilor de informaţii, culegerea datelor din surse umane va I«vrui, la rândul ei, mai importantă.

Plin urmare, *humint* şi *techint* pot avea roluri complementare; nu, iiat, pot oferi diverse tipuri de informaţii. Bineînţeles că prăbumt*; i „Cortinei de Fier" a eliminat motivul iniţial care a stat la baza iv/voltării de către Statele Unite a unui sistem sofisticat de exploatare irhilici. Cu toate acestea, obligaţiile continue de a monitoriza depo-/iirle de arme ale altor state, în special ale celor cu societăţi închise şi programe active de dezvoltare a armelor de distrugere în masă, împreună cu o cerere din ce în ce mai mare de informaţii tehnice din I ui ca Armatei americane pentru sprijinirea operaţiunilor sale, sugerează «.1 este puţin probabilă o îndepărtare substanţială de activitatea de iilegeit a informaţiilor din surse tehnice. De asemenea, necesitatea alegerii anumitor informaţii despre state, actori politici şi preot supări noi este satisfăcută cel mai bine de datele

furnizate de surse umane. Deşi amestecul corect de *humint* şi *techint* va fi, aşa cum a fost şi în trecut, un subiect dezbătut pe larg, este foarte probabil ca o putere globală ca Statele Unite să continue să aibă nevoie de amândouă.

Această discuţie despre *humint* şi *techint* & abordat importanţa fiecăreia pentru culegerea informaţiilor strategice – informaţii destinate factorilor de decizie la nivel naţional. De asemenea, este totuşi important de remarcat că progresele din telecomunicaţii şi IT au făcut posibil ca informaţiile culese de sistemele *techint* (inclusiv cele dezvoltate pentru a fi utilizate la nivel naţional) să fie puse la dispoziţia comandanţilor pe câmpul de luptă în timp real – sau, în orice caz, suficient de rapid pentru a fi utile în scop tactic. Această dezvoltare se află încă la început, dar promite să devină o utilizare importantă a sistemelor *techint92*.

Culegerea informaţiilor din surse deschise

Publicaţii şi emisiuni radio şi TV

Nicio discuţie despre culegerea informaţiilor nu ar fi completă dacă nu s-ar face referire la datele provenind din surse deschise – adică ziare, cărţi, emisiuni radio şi de televiziune, Internet şi orice altă sursă publică de informaţii.

Importanţa surselor deschise în procesul culegerii de informaţii este un subiect de dezbatere şi, în fond, are legătură cu aspecte fundamentale privind categoria informaţiilor. O perspectivă, exemplificată de Sherman Kent, este că majoritatea „activităţilor de culegere a informaţiilor externe eficiente de la nivel înalt...

trebuie să se realizeze prin observaţie şi cercetare deschisă, directă şi realistă" 93. Perspectiva mai tradiţională este că, deşi sursele deschise pot oferi un context şi o bază importante, faptele-cheie, cum ar fi intenţiile exacte ale unui inamic, trebuie obţinute în primul rând, dacă nu exclusiv, din surse care nu sunt publice, apelându-se la spionaj sau exploatare tehnică.

Această problemă este discutată pe larg în capitolul 7. În acest moment, accentul se va pune pe diversele întrebuinţări care pot fi date informaţiilor din surse deschise. De exemplu, o sarcină standard a ofiţerilor din serviciile de informaţii a fost să pregătească compendii

Hltttr ni informaţii privind ţările în care ar putea fi întreprinse în»h... i operaţiuni militare. Teoretic, aceste compendii includ toate h.iMim, iiile ce ar putea fi utile personalului militar. Informaţii privind geografia ţării, reţelele sale de comunicaţii şi transport, Im.»pl, militare şi economice-cheie şi aşa mai departe ar trebui incluse M linul îi suficiente pentru a-i permite celui care elaborează planul n în îi scrie de decizii – de exemplu, să determine cât de repede ar i... a h mutate trupele şi proviziile din punctul A în punctul B.

I îi excepţia celor mai „secretoase" ţări (cum ar fi fosta Uniunea în krlică, ce a recunoscut în 1988 că a falsificat hărţi ca măsură de in Hale) 94, o mare parte din aceste informaţii vor fi disponibile în imiahira surselor deschise: hărţi şi orare rutiere şi feroviare, oiitolc din ziare şi reviste, rapoarte economice şi statistice ale

yiivnmilui şi chiar ghiduri de călătorie vechi. Culegerea şi cata-lny.tH\i lor reprezintă alte aspecte. Sunt implicate volume uriaşe de minimalii şi este puţin probabil să fie disponibile vreodată resursele în i esarc culegerii lor pentru fiecare ţară în parte. Dacă, după cum mult discuta în următorul capitol, forţei militare americane care a noada! Grenada în 1983 nu i-au fost furnizate hărţi corespunzătoare «i alle informaţii despre insulă, motivul a fost nu dificultatea de a iilrjte informaţii, ci nealocarea unor resurse suficiente pentru ceea piohabil că multora li s-a părut a fi o insulă mică, îndepărtată.

În mod asemănător, o gamă largă de surse statistice din toată Imira fac publice date economice. Cu toate acestea, pentru a hotărî dale să fie culese trebuie ştiut ce informaţii sunt necesare. Poate îi nevoie de date economice pentru a susţine formularea politicii piivând comerţul internaţional sau sancţiunile economice, de soluţii pniiiu a face faţă efectelor crizelor şi cartelelor internaţionale (cum îi li Organizaţia Ţărilor Exportatoare de Petrol) şi aşa mai departe. Ahe tipuri de date economice, ca, de exemplu, cele ce ar rezulta din monitorizarea circuitelor financiare, ar putea arunca lumină asupra îi al icului internaţional de droguri. În sfârşit, este posibil să fie în voie de culegerea unor informaţii economice pentru a susţine ni, di/ele politice şi militare. De exemplu, în timpul celui de-al Doilea KA/hol Mondial, economiştii de la OSS* (care lucrau pentru forţele intenc americane din Europa) au folosit o gamă largă de date

* i) SS – Office of Strategic Services, serviciul de informaţii al SUA din l»crioada celui de-al Doilea Război Mondial, predecesor al CIA (n.r.).

economice, în mare măsură publice, pentru a contribui la planificarea unei campanii strategice de bombardamente; obiectivul a fost distrugerea părţilor din infrastructura industrială germană – uzinele petroliere şi de rulmenţi – considerate vitale pentru sprijinirea succesului războiului nazist95. Mai recent, anticipările privind comportamentul sovieticilor la sfârşitul anilor ’80 au fost dominate de întrebări legate de modul în care va afecta această situaţie economică alte domenii strategice. Fiecare dintre aceste necesităţi privind culegerea informaţiilor atrage după sine diferite categorii de date economice.

Pe lângă aceste tipuri evidente de materiale din surse deschise, analiştii serviciilor de informaţii solicită acelaşi gen de informaţii – discursuri ale unor figuri politice proeminente, texte ale unor legi şi rezoluţii, recensăminte şi alte date demografice – care ar fi necesare pentru orice analiză academică a condiţiilor politice sau sociale dintr-o ţară străină; într-adevăr, produsul final poate fi asemănător.

În funcţie de resursele disponibile, un serviciu de informaţii poate culege datele specializate în cantităţi ce ar copleşi un cercetător universitar. De exemplu, o tehnică importantă pentru a înţelege politicile şi procesele de stabilire a strategiilor în sistemele politice „închise” presupune urmărirea carierei unui număr mare de indivizi pentru a identifica oficialii de nivel mediu

care sunt protejaţii sau „clienţii” anumitor lideri. După ce au fost identificate aceste relaţii patron-client, un analist poate, observând promovările şi retrogradările clienţilor, să determine poziţia adoptată de protectorii lor de nivel înalt. A face acest lucru necesită totuşi întocmirea şi menţinerea unei vaste baze de date biografice. Ar presupune parcurgerea tuturor ziarelor importante şi a tuturor emisiunilor de ştiri, înregistrarea fiecărei ştiri care indică promovarea, retrogradarea sau transferarea unui oficial oricare stabileşte legătura între doi oficiali şi introducerea în computer a bazei de date rezultate, astfel încât să devină utilă pentru specialişti. Unui om de ştiinţă sau chiar şi unui institut de învăţământ superior s-ar putea să îi fie greu să întreprindă o astfel de sarcină96.

Informarea realizată de diplomaţi şi ataşaţi militari

Un alt mijloc de culegere a informaţiilor – unul care ar putea fi considerat un amestec de *humint* şi sursă deschisă, deoarece este obţinut de agenţi, dar într-un mod direct şi deschis – ar fi rapoartele un în prezintă diplomaţii şi ataşaţii militari cu privire la evenim, nit «Im ţările în care sunt numiţi în post. Într-adevăr, linia de

— Mi în iţic dintre diplomat şi ofiţerul de informaţii nu a fost niciodată

Util I»iiţia cum afirmă un istoric al diplomaţiei, „uneori, ambasadorii

«…vasal rapid graniţa confuză dintre culegerea legitimă a inforhmhloi şi spionaj, pe de o parte, şi alte activităţi cu o reputaţie putt Mi, pe

de altă parte” 97. Dar chiar şi astăzi, când cele două

...(îi sunt separate, rapoartele diplomatice despre situaţia politică

Mm 1*11.1 gazdă pot conţine informaţii importante pentru orice analiză i... lui,.1 Un diplomat care beneficiază de acces la figurile politice... (m dintr-o ţară sau este un fin cunoscător al istoriei ţării şi al mim nu îi politice ar trebui să poată oferi o evaluare a situaţiei politice în i im* care nu se poate regăsi în mass-media98.

Iu mod asemănător, ataşaţii militari, în măsura în care au acces la i4 ftri i din ţara-gazdă, pot cunoaşte îndeaproape sistemul militar al Mutului respectiv, ca, de exemplu, personalitatea şi competenţa

H«iilor de rang înalt, precum şi modul lor de gândire caracteristic, imiii, icfe lor de vedere privind doctrina militară şi relaţiile cu conlmi nea civilă. În plus, ataşaţii pot fi invitaţi să urmărească exerciţii Miihi, iie sau să ia parte la demonstraţii sau ocazii solemne la care Se ui r paradă de echipamente militare. De asemenea, pot să călătorească în (îi.i-gazdă şi, astfel, să vadă aerodromuri, porturi şi alte baze MMlii, are şi civile de interes99.

Alii? surse umane deschise

I h»loinaţii şi ataşaţii militari nu sunt singurii cetăţeni străini care i/iitM/a ţări şi raportează observaţiile lor. De exemplu, Acordul din

I → K / încheiat între Statele Unite şi URSS privind eliminarea rachetelor ni rarii medie şi

scurtă de acţiune (Tratatul INF) şi, mai recent.

Îi.naiul de Reducere a Armelor Strategice (START) prevăd ca fiecare l ale să trimită inspectori la anumite baze militare ale celeilalte părţi Minru a constata dacă ţara respectivă respectă termenii Tratatului. Îitsjicctorii au un acces mai mare la acele baze decât ataşaţii militari… ui alţi vizitatori. Evident, rapoartele lor vor conţine informaţii îi în roase privind forţele militare ale ţării-gazdă.

Iu mod asemănător, oamenii de afaceri, savanţii şi alte persoane

În călătoresc află informaţii despre ţările pe care le vizitează informaţii care, deşi nu sunt secrete în mod oficial, nici nu suni disponibile în mod public. Pentru ca aceste informaţii să ajungă la guvernul ţării lor, este necesar, într-o ţară ai cărei cetăţeni nu au nevoie de permisiune specială pentru a călători în străinătate, ca aceste persoane să fie dispuse să le transmită. Dar intensificarea generală a comerţului internaţional, a turismului şi a cercetării a însemnat o dezvoltare substanţială în ultimii ani a posibilităţilor privind culegerea informaţiilor din surse umane deschise.

Capitolul 3

Ce înseamnă toate acestea? Analiza şi producerea informaţiilor

Co este analiza?

m.tli/.i se referă la procesul de transformare a informaţiilor care ni «mese în orice mod într-un produs care poate fi folosit de I M h îi de decizie şi liderii militari. Rezultatul sau „produsul inforpolial” poate lua forma unor scurte

memorandumuri, rapoarte iie knie amănunţite, expuneri sau orice alte mijloace de prezentare a imlmimaliilor. Această secţiune arată gama de tehnici analitice. În lezuicrca acestor activităţi, nu este utilizată întotdeauna ter Min.»logia standard a activităţii de informaţii; mai mult decât atât, umil/a nu are categorii standard. În plus, categoriile care există nu mi nici exacte, nici nu se exclud reciproc. Am încercat o aranjare cu luncilor de la cea mai tehnică, precum decriptarea mesajelor, la i mai speculativă, ca, de exemplu, prezicerea viitoarelor ten-iltnr sociale şi politice. Într-o secţiune ulterioară se discută despre illvri sila tea de produse informaţionale şi funcţiile pe care le Unie plinesc.

An.în/a tehnică şi nu/am sintagma *analiza tehnică* aici pentru a ne referi la metodele Mialmcc care transformă datele foarte specializate, total sau aproape

I«neînţeles pentru oricine altcineva în afară de specialist, în date pe nimic pot folosi alţi analişti din domeniul informaţiilor. Exemplele discutate sunt *criptanaliza* (care transformă şiruri aparent aleatorii de litere şi numere într-un mesaj într-o limbă cunoscută), *analiza telemetrică* (transformând un semnal radio într-o serie de valori care descriu capacitatea de zbor a unei rachete sau a unui alt vehicul de testare) şi *interpretarea fotografică* (identificând şi măsurând obiectele dintr-o fotografie).

*Criptanaliza*. Aceasta se referă la rezolvarea sau „spargerea” codurilor şi cifrurilor inamice, prin aceasta permiţându-le analiştilor să readucă

un mesaj criptat interceptat la forma lui iniţială, cu înţeles, în majoritatea cazurilor, interceptarea presupunea receptarea unor semnale radio de către altcineva decât destinatarul lor. Cu toate acestea, problema criptanalitică este aceeaşi în cazul unui mesaj criptat preluat de la un curier capturat, o scrisoare criptată deschisă de cenzura poştală sau o telegramă criptată obţinută prin interceptarea cablului telegrafic.

În uzajul tehnic, termenii *cod* şi *cifru* se referă la metode diferite de criptare. Într-un *cod*, un cuvânt sau o expresie (care semnifică un lucru, un concept sau o locaţie) sunt înlocuite cu un grup de cifre ori litere (care pot sau nu să formeze un cuvânt real), ce se găseşte în dreptul cuvântului sau expresiei respective într-o listă de coduri. Astfel, mesajul *Attack on Saturday* (*Atac sâmbătă*) s-ar cripta prin găsirea grupului de coduri pentru *attack* (să spunem, FGHJ) şi a celui pentru *Saturday* (să spunem, ADFK), producând astfel mesajul criptat FGHJ ADFK. Dacă un cuvânt nu se găseşte în lista de coduri, expeditorul poate fie să reformuleze mesajul pentru a utiliza cuvinte şi expresii care apar în ea, fie să exprime literă cu literă cuvântul lipsă folosind grupuri speciale de coduri pentru litere sau silabe individuale.

În schimb, într-un *cifru*, fiecare literă din mesajul iniţial – numit *text lizibil* – este înlocuită, urmând o formulă sau un algoritm, cu o altă literă, formând astfel *textul cifrat*. (într-un cifru „de transpunere”, literele mesajului original sunt păstrate, dar sunt transmise într-o ordine aleatorie, conform unei scheme.) De exemplu, un

cifru ar putea consta în regulă conform căreia fiecare literă să fie înlocuită cu litera care o urmează în alfabet. În acest cifru extrem de simplu, mesajul din exemplul dat mai sus ar fi cifrat ca BUUBDL PO TBUVSEBZ.

I îi i ihn mai complicat (dar mult prea simplu pentru a oferi lyhi, m (i) ar putea consta în următorul algoritm: se înlocuieşte HtlMUI lucia din mesaj cu litera care o urmează în alfabet; a doua h». i.1 «h litera care se află cu două poziţii mai jos în alfabet; şi aşa mâni «lrp, iile. (în cazul unui astfel de cifru, alfabetul ar fi considerat». ni iun un cerc, cu litera A urmându-i imediat literei Z. Astfel, cea

I Wi.1 literă a mesajului ar fi neschimbată, în timp ce a 27-a, la i i pl, una, ar fi înlocuită cu cea care îi urmează imediat şi aşa mai i. milr) Acum, mesajul ar fi BVWEHQ VV BKEGERPO.

Ai este tehnici pot fi combinate în diverse moduri. De exemplu… m mm’s.i codat poate fi el însuşi cifrat în acelaşi mod în care ar putea fi şi un lexi lizibil. Astfel, mesajul pe care l-am dat drept exemplu, mim i-a mai înainte şi apoi cifrat cu prima metodă discutată – ar *p* în ia următorul text „supercifrat”: GHIK BEGL. Avantajul unei Hill I se proceduri este securitatea sporită pe care o oferă: pentru a N mn-ia mesajul original, un inamic trebuie să spargă atât codul, cât «i llml De obicei, codul rămâne valabil mult timp, iar algoritmul i Umilii se schimbă frecvent. Motivul este că, în timp ce primul este l» ilul de greu de schimbat (fiecare schimbare de cod înseamnă că în. Imme distribuite noi liste de coduri fiecărei ambasade,

baze sau piţir care ar putea să trimită sau să primească mesaje), algoritmul i III-ului este simplu de schimbat.

I *n/nanaliza* este procesul de rezolvare („spargere”) a codurilor îi.i «iliurilor – adică reconstituirea listei de coduri a inamicului sau şi în hurea metodei acestuia de cifrare a mesajelor – folosind, în pimiiil rând, chiar mesajele criptate. (*Decriptarea*, în schimb, se h lua de obicei la procesul prin care destinatarul – care bineînţeles

«i viu* deja codul sau cifrul folosite – recuperează textul iniţial.) i *ninologia* este studiul mai general al acestor aspecte, atât în scopuri npiaiialitice, cât şi în scopul realizării unor coduri şi cifruri mai %iMnc. *Criptografia* se referă uneori la activitatea de realizare a «liniilor şi a cifrurilor, dar este folosită câteodată şi ca sinonim în unu *criptologie*.

Materia primă cu care începe de obicei criptanaliza este o colecţie de mesaje criptate. Sarcina criptanalizei este de a identifica tiparele v i-aenle în amalgamul de litere şi cifre, aparent fără sens, şi a stabili le caiura dintre acele tipare şi tiparele cunoscute, existente în limba în care se presupune că au fost scrise mesajele. De exemplu, în textele obişnuite în limba engleză, litera E este mai frecventă deeai oricare alta; aşadar, într-un grup de mesaje cifrate folosind metoda simplă de substituţie, despre care am discutat mai sus (în care fiecare literă din textul iniţial este înlocuită cu cea care o urmează imediai în alfabet), litera F este probabil cea mai frecventă.

Observând acest lucru, criptanalistul ar trage

concluzia că F îl înlocuieşte pe E. Apoi, el ar putea observa faptul că UIF apare mai des decât orice alt cuvânt format din trei litere, presupunând că îl înlocuieşte pe THE. În acest moment, ar putea ghici şi faptul că fiecare literă în textul cifrat înlocuieşte litera premergătoare din alfabet şi, testând această ipoteză, ar descoperi că este corectă.

După cum se poate vedea din acest exemplu simplu, cantitatea de materie primă pe care o poate obţine criptanalistul este un factor important ce poate influenţa identificarea unei soluţii. Într-un mesaj scurt, E nu apare neapărat în mod frecvent: în exemplul nostru („Atac sâmbăta”) nu apare deloc. Cu toate acestea, într-un mesaj mai lung sau într-o înşiruire de mesaje, se aplică legea probabilităţii. Este puţin probabil ca frecvenţa literelor (sau grupurilor mici de litere) din textul iniţial să difere foarte mult de cea cu care apar în textele obişnuite în limba engleză1.

Istoria criptologiei este fascinantă, dar textul de faţă nu ne permite să intrăm în detalii2. Vom identifica trei perioade, în funcţie de tehnologia existentă pentru criptarea mesajelor.

În prima perioadă, începând din Antichitate şi până în anii ’30, mesajele erau criptate manual. Existau diverse tehnici, liste de coduri, cifruri de transpoziţie şi de substituţie. La sfârşitul acestei perioade listele de coduri cuprindeau mii de articole. Totuşi, din moment ce acestea erau folosite perioade îndelungate, criptanaliştii le puteau reconstitui. În mod similar, pentru obţinerea unui text cifrat, trebuiau efectuate

manual o serie de modificări, ceea ce a redus complexitatea cifrurilor şi a uşurat munca criptanaliştilor. Cu cât algoritmul de criptare devine mai complex, creşte posibilitatea apariţiei unei erori de criptare sau decriptare, de aceea cifrurile mai greu de „spart” nu sunt întotdeauna practice.

Bineînţeles că metoda cea mai uşoară de spargere a unui cod este de a fura sau a obţine prin orice alt mijloc o copie a listei de coduri. Din moment ce crearea unei liste de coduri şi distribuirea ei sunt dificile, codurile erau utilizate o perioadă îndelungată, ceea ce sporea utilitatea listei de coduri.

m cu în iiica Primului Război Mondial, cât şi în timpul acestuia.

111! hilci i ale Europei deţineau birouri speciale unde se decriptau me I«militare şi diplomatice străine. De exemplu, la începutul

…Im Război Mondial englezii au obţinut (de pe navele capturate mm –, Mlmidate) copii ale principalelor liste de coduri maritime pttti Mtr e germanii au luat măsuri suplimentare de siguranţă, criptând ne le deja codate; cu toate acestea, britanicii au reuşit să le lhr/ev

Inlmsi, cel mai important succes criptanalitic englez l-a reprezentat. Naica codurilor folosite de diplomaţia germană. La data de îl ianuarie 1917, criptanaliştii britanici au descifrat un mesaj, Hinwill în istorie drept „telegrama Zimmermann”, prin care mmmmiii de Externe german i-a transmis instrucţii ambasadorului uimii din Mexic cu privire la o posibilă alianţă germano-mexicană

i»m... iiiva Statelor Unite, în cazul în care americanii ar fi răspuns la... i se germane submarine (programate pentru 1 februarie), decla

— Lml ia/l»oi Germaniei. Decizia Preşedintelui american Woodrow WII mhi de a declara război a fost influenţată decisiv de publicarea în Mâni le din SUA a telegramei din care se deducea că Mexicul inten!* im.t/a’s; l recupereze Texasul, New Mexico şi Arizona. Iscusinţa

...e a fost publicată telegrama nu a dat de bănuit părţii germane lim fi fost posibilă spargerea codului utilizat4.

mic deosebire de europeni, la începutul Primului Război Mondial mim i m.mii nu aveau încă experienţă în domeniul criptografiei. Istoria iipit»mafiei americane din timpul războiului şi din următorii zece mm, maia cum, în ciuda provocărilor intelectuale deosebite, încă era lt»il ca un specialist, lucrând pe cont propriu sau cu un grup h Mi Ans de colaboratori, să descopere principiile fundamentale ale npiaiii, precum şi coduri şi cifruri folosite pentru criptarea celor m, în importante mesaje. Herbert Yardley povesteşte cum, lucrând de iiitil singur, a reuşit să criptanalizeze un mesaj trimis preşedintelui M IImhi de colonelul Edward House, delegatul personal al lui Wilson, nilul în momentul respectiv în misiune diplomatică în Germania A. Ni Lilarca lui Yardley despre perioada în care s-a aflat la conducerea li pai lamentului de criptanaliză al armatei Statelor Unite, în momentul Minai îi acestora în război, precum şi a „Black Chamber”

din cadrul l» pai lamentului de Stat după încheierea războiului, indică faptul că li al ei moment criptografia era mai degrabă o artă decât o ştiinţă şi

J

În ce măsură perspicacitatea şi intuiţia specialiştilor a influenţai acest domeniu.

Totuşi, în criptologie, ca şi în alte domenii ale activităţilor militau-şi de informaţii, Primul Război Mondial a reprezentat o etapă esenţială. Conform unui istoric:

Primul Război Mondial a marcat punctul de cotitură în istoria crip tologiei. Înainte de război, domeniul era limitat; după încheiere» războiului, acesta a luat amploare. Războiul a marcat dezvoltarea acestei ştiinţe. Principalul motor al acestei evoluţii a fost creşterea semnificativă a nivelului de comunicaţii radio6.

Spargerea unui cod sau cifru utilizat de inamic reprezenta un avantaj semnificativ în condiţiile creşterii traficului radio. În acelaşi timp, un trafic mai mare sporea vulnerabilitatea codurilor şi cifrurilor de o complexitate similară faţă de metodele de criptanaliza; deoarece, existând mai multe mesaje (criptate cu acelaşi cod sau cifru), criptanalistul avea mai multe şanse să identifice tiparele repetitive care permit găsirea unei soluţii.

Traficul radio sporit ducea la supra-încărcarea sistemului manual de criptare şi decriptarea. Acest lucru, coroborat cu necesitatea unor sisteme de criptare mai sigure, a reprezentat cea de-a doua perioadă din istoria acestei ştiinţe

în care aparatele mecanice şi electromecanice, cum ar fi maşina de criptare americană Hagelin, Enigma germană şi maşinile japoneze Purple (Maşina de scris alfabetică 97) au fost folosite pentru a cripta texte.

Astfel de maşini puteau utiliza algoritmi şi formule mult mai complicate decât cele folosite în perioada în care criptarea se realiza manual. Prin urmare, tehnicile şi procedurile criptanalitice atingeau un nivel de complexitate similar. Spargerea codurilor a necesitat crearea şi utilizarea primelor maşini de calcul şi a determinat progrese în statistică şi în alte ramuri ale matematicii teoretice7. În timpul celui de-al Doilea Război Mondial, s-a scris un număr impresionant de articole despre maşinile electromecanice de criptare, cum ar fi Enigma şi Purple8.

Ne aflăm în prezent în cea de-a treia perioadă din istoria acestei ştiinţe care este caracterizată de utilizarea computerelor pentru criptarea şi decriptarea mesajelor şi în sprijinul eforturilor criptanalitice.

...I «vident, acesta este un subiect foarte sensibil despre care

I ni mi arc foarte multe informaţii. Dezvoltarea „criptografiei Miltlii, studierea şi folosirea criptografiei de către oameni de TMIMţa nu oameni de afaceri independenţi – a furnizat publicului un i *în* mare de informaţii despre acest domeniu9. Totuşi, nu este. a.îi ia coniparăm metodele criptografiei publice cu cea a agenţiilor itv minimalii, bazându-ne doar pe surse publice.

I în male acestea, pot fi prezentate situaţia actuală şi punctele, im ale anumitor ţări în domeniul criptologiei. Date fiind rolul m. Mieielor şi monopolul deţinut de SUA în domeniul IT, concluzia 4. h. I americanii au un avantaj în procesul de decriptare; într-o 4 m. MMIIA măsură, această influenţă poate fi contracarată de progresele aale (de exemplu, ale Rusiei) în domeniul matematicii teoretice. Im a» el a. Şi timp, s-ar părea că progresele în domeniul IT (în ceea pl, ixrsie viteza cu care se efectuează operaţiile aritmetice de bază) NvMM/r.i/a domeniul apărării. Cu alte cuvinte, deşi progresele în

...nul IT permit atât celui care criptează să folosească cifruri cu

...ad mai ridicat de complexitate, cât şi criptanalistului să le

...iMtiMiie/e, avantajul este de partea celui ce realizează criptările, îi»nsele din domeniul IT permite obţinerea unor cifruri mai

HMiple.u» pe care aceleaşi computere nu le pot sparge. Dacă aceasta» I«Miuaiia, pe termen lung, criptanaliştii nu au şanse foarte mari de «ipaiee cifrurile marilor puteri utilizând cea mai avansată teh

— L» în ic în domeniu. În practică, desigur, dacă din cauza unei erori în

Mitlirmare nu este utilizată pe deplin tehnologia computaţională i» mila în realizarea unui cifru, acesta va fi mai vulnerabil. În plus, i noi, uialiştii pot profita de utilizarea greşită a unui cifru pentru a-l paire10. Agenţii pot furniza listele

de coduri ale inamicului, i»…uni de criptare, astfel permiţând unei serviciu de informaţii să le i iipicze mesaje ale căror sisteme de criptare nu au putut fi sparte I’hm *i* i iptanaliză”.

I *ulnerabilitatea criptanalizel.* Criptanaliza este una dintre cele hihi li agile metode ale serviciilor de informaţii, deoarece ţările pot. Imiiha sistemul de criptare în momentul în care îşi dau seama că… mucul le poate descifra mesajele. Astfel, nu este surprinzător ipint că succesele criptanalitice ale americanilor şi englezilor din MMipul celui de-al Doilea Război Mondial s-au numărat printre cele mai importante secrete de război, beneficiind de cel mai înalt gâtă de securitate. Englezii au ţinut secret timp de 30 de ani faptul că au descoperit modul de funcţionare al maşinii de criptat germane Enigmi, în ciuda numărului mare de oameni implicaţi în operaţiune.

Experienţa americană a fost foarte diferită. Publicarea la data d 7 iunie 1942 a unui articol de către *Chicago Tribune* despre victoiiu americanilor în Bătălia de la Midway a reprezentat una din cele mi grave breşe de securitate din timpul războiului. Intitulat „Forţer navale au aflat de un posibil atac japonez”, articolul cita materialo rezultate din mesajele japoneze decodate. Acestea au cuprins nu doar numele transportoarelor japoneze implicate, ci şi ale cruci şătoarelor care sprijiniseră forţele de ocupaţie. În plus, articolul susţinea că, atunci când flota japoneză a înaintat spre Midway, „toate avanposturile americane au fost avertizate” şi că serviciile de informaţii ale marinei americane au

anticipat „un atac simulat la o bază americană [Dutch Harbor, în insulele Aleutine], care avea st fie însoţit de încercări importante de invadare şi ocupare a altei bazo militare [insula Midway]”12.

Un expert japonez în informaţii ar fi conchis în urma articolului că Statele Unite au avut acces la mesajele japoneze codificate privind acţiunile maritime. Problema a fost prezentată în faţa juraţilor Curţii din Chicago; totuşi, niciunul dintre inculpaţi nu a fost pus sub acuzare. Se pare că înalţi funcţionari ai administraţiei americane s-au pronunţat împotriva urmăririi injustiţie a inculpaţilor, pe motivul că un proces ar atrage atenţia asupra articolului şi probabil ar fi fost necesară o confirmare publică a faptului că americanii citeau mesaje japoneze codate privind acţiunile maritime. (Ca o ironie, la data de 31 august 1942 un congresman a menţionat acest lucru într-un discurs criticând aspru felul în care ziarul *Tribune* „s-a folosit în mod greşit şi nechibzuit de libertatea presei”) 13.

Încă nu se ştie dacă japonezii au beneficiat sau nu de pe urma acestei „scurgeri” de informaţii. Este adevărat că la data de 14 august 1942 Marina japoneză a introdus o nouă versiune a codului (numit de către criptanaliştii americani JN-25 d). Apariţia unei noi versiuni a codului la atât de scurt timp după introducerea (la 1 iunie) a versiunii anterioare (JN-25 c) ridica suspiciuni”. Totuşi, noua versiune a codului „păstra caracteristicile formulei extinse JN-25”, permiţând astfel Statelor Unite să aibă din nou acces la mesajele

…/*i* mult mai uşor decât dacă japonezii ar fi introdus un sistem ml în»ar\ Cu toate acestea, Statelor Unite le-a luat patru luni putui.1 cunoaşte codul JN-25 d la fel de bine ca pe versiunea «mi, hmiia1.

I în cu iuplu mai clar de vulnerabilitate a criptanalizei, care pl. «tic de data aceasta Marea Britanie, datează din anul 1927. În… m (micdenţi, biroul criptanalitic englez, Government Code and

Im i şi hool, a reuşit să decripteze mesajele transmise între sediul

…iici îi (Internaţionala Comunistă) şi Guvernul sovietic din Moscova.

I» il* o p.iiie, şi diferiţi reprezentanţi sovietici la Londra – Ambasada iuţi picctim şi o comisie comercială şi un birou comercial al Arcos, I mici Cooperatistă Rusă –, pe de altă parte. Astfel, Guvernul»m-le /.1 urmărit activitatea diplomaţilor ruşi şi ale delegaţilor comerciali, în ut, ludea spionajul şi implicarea în activitatea sindicatelor engleze. Im.hml 1927, englezii au invocat încălcarea uzanţelor diplomatice, imih mp and legăturile cu Uniunea Sovietică. Datorită faptului că în Ivtil, iinciil s-a solicitat argumentarea acestei decizii, miniştrii englezi… iii / valuit public faptul că aveau capacitatea de a decripta mesajele… mhihe. După cum era de aşteptat, Uniunea Sovietică a introdus m… i iliuri, pe care englezii nu au reuşit să le spargă17.

H îi caz asemănător, în care un guvern ales în mod democratic a»tv/v.iliiit tipul de capacităţi criptanalitice deţinute în scopul de a i.pnc sprijin pentru politicile sale, dar a pierdut în acelaşi timp

raliulmitea de decriptare a mesajelor, se pare că a avut loc în milde Unite în anul 1986. Pentru a justifica eventuala decizie de a... mluida clădirile guvernamentale din Tripoli, Libia:

hi şedinţele [Ronald] Reagan [conform *The Washington Post*] şi cei mai minirtanţi consilieri ai săi au făcut o extraordinară dezvăluire privind mlorinaţiile sensibile... pentru a demonstra că Statele Unite aveau dovada.i Libia... era direct responsabilă pentru bombardarea unui bar de imupie din Berlinul de Vest...

IMnliile prezentate de preşedinte[,]... relatează sursele, vor evidenţia l.ipiul că Statele Unite pot să intercepteze şi să decodifice comunicaţiile liplomatice ale Libiei18.

I Mipă cum era de aşteptat, „dezvăluirea publică a capacităţii de I... «mare a comunicaţiilor diplomatice libiene a dus la pierderea unei m.e de informaţii valoroase pentru analiştii de informaţii americani, a cărei înlocuire va dura săptămâni sau chiar luni întregi, au declari! astăzi oficiali din Administraţie" 19.

Aceste exemple vin în sprijinul unei teorii generale despre informaţiile secrete care se poate aplica şi în cazul altor tehnici dl analiză şi culegere: cu cât sunt mai valoroase informaţiile existente, cu atât se manifestă mai multă reticenţă în utilizarea lor şi probabil acest lucru atrage atenţia inamicului asupra capacităţilor de culegere a informaţiilor. În cazul unui guvern democratic, dilema este cu al Al mai mare cu cât acesta se vede nevoit să dezvăluie informaţii despre metodele sale de culegere a datelor pentru

a convinge opinia publică de faptul că strategia sa de guvernare este fundamentată. Dar orice guvernare se confruntă într-un fel sau altul cu această dilemă atunci când deţine informaţii secrete pe baza cărora intenţionează să acţioneze.

Cel mai probabil, această problemă poate apărea pe timp de război, când impulsul de a acţiona pe baza acestor informaţii este foarte puternic. De exemplu, în timpul celui de-al Doilea Război Mondial englezii cunoşteau, din interceptarea şi decriptarea comunicaţiilor, traseul exact al navelor germane care transportau provizii pe Mediterană, pentru forţele generalului Erwin Rommel aflate în Africa de Nord. Cu toate acestea, pentru a nu le trezi suspiciuni germanilor în privinţa securităţii comunicaţiilor, englezii acţionau conform regulii care prevedea că nicio navă nu poate fi atacată înainte de a fi survolată de aeronavele de recunoaştere, astfel acordându-le germanilor o explicaţie despre modul în care englezii au reuşit să le identifice navele.

Acest punct de vedere este ilustrat şi de faptul că, din câte se pare, prim-ministrul britanic Winston Churchill aflase de raidul aerian german nimicitor asupra oraşului englez Coventry înainte ca acesta să se producă, dar nu a luat nicio măsură pentru a avertiza apărarea antiaeriană sau serviciile de urgenţă, de teamă să nu compromită capacităţile britanice de decriptare a mesajelor Luftwaffe. Cercetărilor istorice au infirmat această ipoteză: informaţiile culese prin interceptarea comunicaţiilor nu le-au permis englezilor să identifice Coventry drept ţinta atacului20. Totuşi,

povestea oferă o descriere destul de dramatică a dilemelor morale şi strategice cu care un guvern *s-ar putea* confrunta pentru a decide dacă ar trebui să rişte o sursă de informaţii folosind datele oferite de aceasta.

*Sttiih.a* (*elementrică*. Telemetria reprezintă transmiterea radio a mie»imaţii de la un vehicul-test către o staţie de la sol – inlhi m.i (îi privind funcţionarea vehiculului (de exemplu, acceleraţia mm li h de la propulsie a motorului), starea acestuia (cum ar fi»imn rulursi diferitelor componente sau numărul de vibraţii înre-şUM.m sau alte caracteristici. Scopul constă în furnizarea datelor ne inginerilor care efectuează testul, pentru a evalua perii în mania vehiculului său, în caz de eşec, pentru a determina cauza

Miilm IV baza acestor informaţii, inginerii reconstituie profilul de!…», îl vehiculului şi se asigură de siguranţa acestuia ori fac alte m.m. IIIH ari necesare.

Ioiiisi, aceleaşi semnale radio pot fi interceptate de către un – vii ui de informaţii străin printr-o metodă numită informaţii din mI.mhiiic ori *telint*. Analiza telemetrică este procesul prin care Mii le *lehnt* sunt folosite pentru a deduce caracteristicile de bază ale

…h velucul-test. Desigur, în momentul în care inginerii care efec

…/a lesiul încep să interpreteze datele, ştiu deja, din structura

— Le mului telemetrie, la care dintre caracteristicile rachetei se referă h», ale parte din fluxul de sistem (sau „canalul” telemetrie). În».

lumii, analiştii de date din telemetrie aflaţi în slujba unui serviciu – n im mi deţin astfel de informaţii la început; trebuie să stabilească h h.i/a informaţiilor radio care este caracteristica măsurată de *tU* ale canal21. Odată ce au fost stabilite aceste aspecte, analiştii pot im… na să creeze un model de rachetă pe computer, de unde să.i.iive/e caracteristici cum ar fi greutatea iniţială (greutatea de Mttturc) şi încărcătura utilă (focosul „greutatea de aruncare”).

Pentru a fi la curent cu ultimele noutăţi privind programele de.m manient strategic ale Uniunii Sovietice şi a monitoriza respectarea, li i”. ic Moscova a acordurilor de control al armamentului s-a utilizat îi. În/a telemetrică. Totuşi, asemeni criptanalizei, analiza telemetrică pu / mia vulnerabilităţi. În momentul în care un guvern înţelege cât li iMiportante sunt informaţiile telemetrice privind programul de un, în mare al unui inamic şi identifică modalitatea în care ar putea fi în le se datele telemetrice privind propriul program, acesta poate lua mumii i pentru prevenirea scurgerii acestor informaţii. De exemplu, în miipul dezbaterilor de ratificare a SALT II, în anul 1979, a devenit l-ai laplul că Statele Unite s-au bazat în principal pe datele telemetrice l liuiiic de la sovietici pentru a monitoriza programul de înarmare cu rachete şi pentru a verifica în ce măsură ruşii respectau acordul. În plus, până la sfârşitul anilor ’70, serviciile de informaţii sovietice ajunseseră, prin intermediul spionajului, să cunoască detaliul modalitatea în care Statele Unite culegeau din

spaţiu date telemetrice privind rachetele sovietice. Indiferent de motive, din acel moment, Uniunea Sovietică a codificat informaţiile obţinute prin telemetrie în urma testelor cu rachete, împiedicând accesul serviciilor secrete americane la aceste informaţii22.

Nu se ştie în ce măsură este posibilă criptanaliza datelor codificate din telemetrie. Există şi alte metode în afară de criptare pentru a bloca accesul serviciilor de informaţii adverse la informaţiile din telemetrie. După cum am arătat în capitolul precedent, datele pot fi stocate pe o bandă în interiorul unei capsule cu înveliş de protecţie (asemănătoare „cutiei negre" instalate pe aeronavele comerciale) care nu este distrusă în contact cu atmosfera şi în momentul impactului cu solul şi care poate fi recuperată de la bordul vehiculului. În mod similar, datele telemetrice dintr-o rachetă de croazieră sau un avion experimental pot fi transmise la o tensiune joasă către un avion de „urmărire" care zboară aproape şi înregistrate la bord; dacă semnalul radio este destul de slab, acesta poate fi imposibil de interceptat din afara zonei de test.

*Interpretarea foto*. În ciuda echipamentului sofisticat care poate face fotografii în interiorul unui teritoriu inaccesibil, nu s-a descoperit niciun instrument mai eficient decât ochiul uman pentru studierea fotografiilor. Aceasta nu este o sarcină atât de uşoară pe cât pare; deşi deseori se spune că fotografiile sunt o formă de informaţii secrete foarte convingătoare (în sensul că înalţii oficiali sunt mai siguri de informaţiile primite atunci când

„le văd cu ochii lor”), fotografia de supraveghere obişnuită este probabil indescifrabilă pentru un amator. Abia după ce analistul foto {*photo interpréter* PI) identifică aspectele de interes, acestea vor deveni clare şi pentru cei care nu sunt de specialitate23.

Calitatea unui sistem fotografic de recunoaştere este de obicei evaluată în funcţie de ceea ce numim „distanţa de rezoluţie de la sol”. Acest termen tehnic defineşte mărimea celui mai mic obiect care poate fi identificat dintr-o mulţime de obiecte sau din fundal. Deşi mulţi alţi factori trebuie luaţi în calcul pentru a determina cât

». Îiir *HK**ic* şi interpretată o fotografie, distanţa de rezoluţie de la i st» „lotuşi... o metodă convenabilă pentru a face o comparaţie şi ihmrc aproximativă” 24. Pe măsură ce rezoluţia de la sol creştet I mii i şi numărul de informaţii ce pot fi extrase dintr-o fotografic. Im? iM-ial, calitatea unei fotografii este evaluată în funcţie de tipul Mtll/r! arc se poate aplica respectivei ţinte. De exemplu, poate fi ui un aparat de zbor (cum ar fi un avion), se poate face o îţi» miilk arc aproximativă (identificarea unui anumit tip de avion), o Mi nuli, arc exactă (stabilirea unei anumite variante a acelui tip de

.”Mi s-au (în scopul analizei tehnice) se poate face o descriere ilimă”?

I hsiaihcle reale de rezoluţie de la sol pe care le pot obţine sateliţii i. Mipiaveghere fotografică ai unui serviciu de informaţii sunt în cu întrucât aceste informaţii le pot indica inamicilor ce tip de Muhl Ale echipament militar, facilităţi ş.a.m.d.) pot

vedea sau nu i.v h ale Astfel de informaţii îi sunt utile oricărui strateg militar în iloreşte să păstreze secretul asupra anumitor detalii ale noilor

1IM1 ine de armament. Aceste informaţii s-ar dovedi utile şi în cazul iihşiilor care elaborează strategiile de dezinformare, deoarece N 11 pMica indica în ce măsură ar fi posibilă diferenţierea între un îmi i real şi unul fals prin procedurile de supraveghere fotografică.

I H în al de bună ar fi rezoluţia, dintr-o fotografie nu pot fi extrase illiihl luate tipurile de informaţii. Analiştii fotografici trebuie să lu', le/e pe baza a ceea ce numim „semnături" – detalii specifice hm în funcţie de experienţă sau logică, sunt asociate cu anumite i. Împăinente, activităţi, intenţii de a lua măsuri în viitor şi aşa mai a. p.îi în De exemplu, extinderea pistei unui aerodrom ar fi necesară în a/ni aterizării unui nou tip de aeronavă; bazându-se pe expe

...la, un analist ştie că lungimea pistei este corelată cu prezenţa

Muni anumit tip de aeronavă şi ar putea conchide că o astfel de in h ia vu va staţiona pe acel aerodrom. În mod asemănător, analiştii mi Mitlitt la concluzia că diferenţa dintre o bază militară sovietică şi mim» libaneză constă în forma de teren de fotbal a uneia faţă de forma în irren de baseball a celeilalte.

Una dintre metodele de utilizare a semnăturilor pe care s-au /.II Statele Unite se numeşte „crateologie" – corelarea echiţi Mileniului militar cu tipul şi mărimea avioanelor care sunt folosite i» îi, iiisport. Odată determinat

faptul că un anumit avion sau o anumită rachetă a fost transportată în avioane de o anumită mărime, conform principiilor crateologiei, se sugerează că şi în alte con tainere de aceeaşi mărime al căror conţinut nu a fost monitori/îţi direct pot exista acelaşi tip de avioane sau rachete27.

Utilitatea semnăturilor derivă din tendinţa multor organizaţii – În special cele militare – de a urma o rutină, de a face lucrurile „ca lit carte”. Astfel, când, în anul 1962, Uniunea Sovietică a decis să îndrepte rachete balistice cu rază medie şi intermediară de acţiune (MRBM – Medium Range Ballistic Missile, cu o rază de acţiune de 1.000 – 3.000 de km – şi IRBM – Intermediate Range Ballistic Missile, cu o rază de acţiune de 3.000 – 5.000 de km) spre Cuba, aceasta «pregătit un sistem de apărare prin amplasarea artileriei antiaeriene în formă trapezoidală de-a lungul coastei cubaneze, iar experţii militari au identificat imediat acelaşi tipar care se aplică şi în cazul rachetelor sovietice SĂ-2 (sol-aer). Această descoperire a atras atenţia serviciilor de informaţii americane cu privire la faptul că pe insulă „se întâmpla ceva extraordinar”. În paralel, informaţiile obţinute în urma monitorizării unei misiuni U-2 care a avut loc ulterior au indicat că în Vestul Havanei aveau loc lucrări masive de excavare şi de construcţie. Cu toate că experţii nu au identificat la faţa locului rachete sau echipamentele pentru rachete, era sigur faptul că sovieticii plănuiau să construiască o bază pentru rachete IRBM, pornind de la modelul de construcţie şi excavaţie. Într-adevăr, când unuia

dintre experţi „i-au fost arătate fotografiile de la bazele din Cuba, el a arătat un manual de operaţiuni al unei astfel de baze aflate în Rusia [IRBM] în Rusia” 28.

Utilizarea semnăturilor poate să fie foarte eficientă, dar şi să dea naştere şi la multe erori. În timpul crizei rachetelor din Cuba, locaţia focoaselor nucleare ale rachetelor a reprezentat o informaţie crucială. Fuseseră deja trimise în Cuba şi, dacă da, unde erau? Utilizând semnături rezultate din fotografii ale instalaţiilor nucleare din Uniunea Sovietică, experţii americani au asociat depozitele de armament nuclear cu măsuri de securitate extinse şi elaborate. Întrucât armamentul a fost utilizat pentru prima dată în afara Uniunii Sovietice, era normal ca focoasele să fie controlate cu şi mai mare stricteţe. Prin urmare, datorită absenţei oricăror activităţi stricte de monitorizare a bazelor de lansare sau a buncărelor pentru depozitarea armamentului aflate în construcţie, experţii au ajuns la concluzia că focoasele nu luaseră încă drumul Cubei.

Imlusi. În timpul evenimentelor, s-a trecut la o analiză mai 4 fH-iitiii (îi; i-a fotografiilor care a dezvăluit faptul că focoasele se jIUmi.i ife la bun început acolo, depozitate în camioane aparent iţind iiMve în lipsa unor elemente care să identifice luarea unor metilii speciale de securitate a zonei sau vreo activitate în jurul l. Iu* ulcior, analiştii nu au semnalizat camioanele sau le-au clasificat în uimi generic drept vehicule pentru transportarea diverselor tipuri» «V itii bric. Abia mai târziu aceste camioane au devenit

elemente de mmoiiia importanţă, făcându-se legătura cu dispunerea armamentului «leu sovietic de Rusia şi Europa de Est29.

Iu plus, dacă adversarul identifică semnăturile pe care se bazează M«itn, el le poate folosi în avantajul său, inclusiv pentru planuri de hm isuine. Conform anumitor relatări, Guvernul indian s-a bazat pe 4 – 1I11 de informaţii pentru a ascunde de serviciile secrete americane *m*» uinic pentru testele sale nucleare din anul 1998. Datele pe care 1 Mivei nul indian le culesese în legătură cu semnăturile pe care se im/mi Staiele Unite proveneau în urma analizei unui incident ce a *41* în h h cu trei ani înainte, moment în care India plănuia să efectueze «ic nucleare. Ca măsură diplomatică iniţiată de către Statele Unite în vetteret dejucării planurile Indiei, administraţia americană a i-piu al care au fost motivele îngrijorării referitoare la iminenţa

1«mai 11 unor teste nucleare; în cadrul acestui demers, specialiştii. În ani le-au arătat oficialilor indieni fotografii captate din satelit 1 mi, iialau indicatorii specifici (semnături) unui test nuclear iminent. Asilcl. s-a dovedit că în anul 1998 Guvernul indian avea mai multă

«pei ienţă în a masca pregătirile pentru un test nuclear (de exemplu, în/îi»pai) d cablurile care făceau legătura între centrul de control şi uiipi, isamentul de testare) 30.

luncile de date (cercetarea de bază)

I»iipa cum am prezentat deja la secţiunea despre culegerea informaţiilor lui surse deschise, o funcţie importantă şi frecventă a serviciilor de

mii hmaţii este reprezentată de asamblarea şi întreţinerea bazelor 111411 de date, care acoperă probleme importante pentru politica niiiaia şi externă a guvernului. Această activitate poate consta în ili/area unor baze de date cu informaţii relevante despre toate Hule unde ar putea avea loc o activitate militară31. Astfel de compendii au scopul de a deveni un instrument de lucru pentru strategii militari, care privesc ţara ca pe o posibilă zonă de luptă. Şi care conţin informaţii detaliate despre forţe militare existente, facilităţi militare şi de transport, topografie militară, precum şi despre politica, demografia, industria şi agricultura ţării.

Deşi problemele analitice care apar atunci când se realizează o asemenea bază de date sunt minime, este necesar să se ştie care informaţii sunt importante şi care nu. Deciziile cu privire la ţările care urmează să reprezinte un viitor teatru de operaţiuni, precum şi gradul de dificultate pe care îl implică aceste activităţi au consecinţe foarte importante în caz că informaţiile cuprinse în compendiu vor fi susţinute de operaţiuni militare. De exemplu, planul prin care Statele Unite şi membrii Organizaţiei Statelor Est-Caraibiene* urmau să invadeze Granada a avut un ritm foarte rapid de evoluţie. O consecinţă negativă a fost faptul că nu erau disponibile hărţi militare adecvate. Conform afirmaţiilor amiralului Wesley McDonald, comandantul forţelor americane în Atlantic, „armata, în special trupele terestre, au folosit iniţial hărţile drumurilor sau alte tipuri de hărţi, ceea ce făcea dificilă determinarea... coordonatelor reţelei. Aceasta

este una dintre lecţiile pe care le-am învăţat” 32.

Alte tipuri de bănci de date sunt puse la dispoziţia analiştilor de informaţii. De exemplu, după cum am arătat deja, culegerea şi analizarea unui număr mare de informaţii nesecrete pot contribui la o mai bună cunoaştere a unei societăţi închise, cum sunt fosta Uniune Sovietică, China şi Coreea de Nord. Documente conţinând date biografice (referiri din ziare cu privire la partide şi oficiali ai guvernului, poziţiile lor, promovări, călătorii şi aşa mai departe), de exemplu, pot fi analizate pentru a clarifica relaţiile lor cu oficiali, luptele interne în cadrul partidelor şi alte aspecte de acest gen.

Elaborarea informaţiilor finite

Tipurile de analiză pe care le-am descris mai sus reprezintă paşii iniţiali necesari în procesul analitic; în cea mai mare parte, rezultatele acestei munci servesc drept sursă pentru alţi analişti de informaţii, dar nu ajung direct la factorii decizionali sau la comandanţi (utilizatorul final al informaţiilor). Această secţiune prezintă tipurile de

— Organization of Eastern Caribbean States – organizaţie creată în 1981 (n. r.).

I *h* MMN linişte produse. Tehnicile folosite nu sunt nici atât de rigide im, am 4 liptanaliza sau analiza telemetrică şi nici la fel de originale 14.4«livilalca de culegere a informaţiilor. În unele cazuri, cum ar fi»! *!»i, tu\i unor informaţii economice şi politice, tehnicile nu pot fi Îi.iimmde acelea corespunzătoare ştiinţelor sociale.

*htf, ar mafii ştiinţifice şi tehnice*. În timpul şi

imediat după cel V»I I Niilca Război Mondial, a crescut gradual ritmul în care au fost ommil, ilc noile principii ştiinţifice şi tehnice destinate domeniului mmlm.h Capacitatea militară a unei naţiuni s-a fundamentat pe Miih, iiea tehnologică şi pe capacitatea de producţie a sistemelor Ntlltluir ce încorporau acea tehnologie, pe capacitatea generală de intuim ţie, pe dimensiunea forţei sale militare şi pe orice alt element m-leiinţă în domeniul militar. Acest lucru era valabil în mod ml în cazul unui război aerian, domeniu care a cunoscut... m.mlu, crea radarului aerian, a sistemelor de navigaţie sofisticate i-i mii în ghidarea bombardierelor către ţintele lor, a avioanelor cu h i", a rachetelor balistice şi de croazieră şi, în final, a bombei m» «mim e Astfel, culegerea informaţiilor cu privire la sistemul militar îi i „în îi de inamic a devenit un obiectiv important pentru agenţiile de in mi îi, ne ale fiecărei ţări. A devenit important să se obţină informaţii le mlmic despre modul de funcţionare al unui sistem în vederea i»le Miilicării metodelor de contracarare.

Ai est lucru a impus o nouă sarcină serviciilor de informaţii, şi Muiiie anticiparea apariţiei noilor tehnologii şi cunoaşterea modului îmi de funcţionare în vederea contracarării lor33. Prin urmare, agenţiile ilt ml urmaţii au solicitat acces la informaţii ştiinţifice şi tehnice m-i i.în/ale şi au cerut ca această capacitate să fie integrată în imn esul informatic.

Activitatea de culegere a informaţiilor din domeniul tehnic şi iMMtţiik trebuie să fie mai

detaliată decât orice altă activitate de Mliycre a informaţiilor pentru ca un cititor neavizat să ştie unde să i «.mie. Aceasta înseamnă că este nevoie de o colaborare strânsă unic analişti şi ofiţerii de teren. Procesul trebuie să fie similar im unici ştiinţifice în care ipotezele (formulate de către analist) sunt»le Mionstrate mai degrabă prin observaţii directe decât prin expenucul. De exemplu, R.V. Jones, şeful departamentului de informaţii i Ministerului Aviaţiei din Marea Britanie din timpul celui de-al iMilca Război Mondial, povesteşte cum teoria sa privind natura primului sistem de semnale radio(*Knickebein*) folosit de către germani ca instrument de navigaţie pentru bombardiere a fost confirmată în momentul în care un avion echipat cu receptoare speciale, ce zbura într-o anumită zonă desemnată de el, a recepţionat semnalele radio pe care a prezis că le va capta în acea zonă34.

Analiza în domeniul informaţiilor ştiinţifice şi tehnice necesită combinarea informaţiilor cu expertiza ştiinţifică sau tehnică. Deşi principiile ştiinţifice sunt prin natura lor universale şi cunoscute de către experţii din întreaga lume, modurile în care sunt aplicate pot diferi de la o ţară la alta. Astfel, acest tip de analiză necesită un grad înalt de cunoaştere a progreselor tehnice şi ştiinţifice în vederea identificării modului de acţiune al inamicului, combinat cu destulă imaginaţie pentru a realiza că inamicul poate soluţiona probleme tehnice pe care propria ţară a analistului nu a reuşit să le rezolve sau chiar să ajungă la o soluţie diferită, dar validă.

*Informaţii militare*. Acestea sunt informaţiile referitoare la bazele militare străine folosite în scopul planificării operaţiunilor militare ale unei ţări pe timp de pace sau al derulării lor pe timp de război. Cea mai elementară informaţie militară este cea pe care o numim „ordine de luptă”, o serie de informaţii primare despre forţele militare ale unei ţări – numărul de soldaţi şi tipurile de arme, structura organizaţională şi alte date asemănătoare. Caracterizarea acestei informaţii drept elementară nu înseamnă că este uşor de obţinut sau că e uşor de ştiut care este numărul trupelor auxiliare sau al rezerviştilor. Revizuirea ordinii de luptă nord-coreene de către serviciile de informaţii americane la sfârşitul anilor ’70 este un astfel de caz; peste un an, estimările informative ale numărului trupelor terestre nord-coreene au crescut cu o treime. Ajustări similare au fost făcute şi în ceea ce priveşte numărul de tancuri, lansatoare de rachete şi „tuburile” de artilerie.

O completare necesară la ordinea de luptă ar putea fi reprezentată de informaţii cu privire la aspectele calitative ale unui amplasament militar străin: calitatea instruirii, calitatea actului de comandă şi alte aspecte asemănătoare.

Mult mai importante decât aceste informaţii fundamentale sunt cele referitoare la metodele de luptă ale forţelor armate: tactica pentru care au fost instruiţi şi pe care au adoptat-o, sub ce formă se

I MMMII rsia războiul plănuit şi ce strategie vor adopta. Datele brute mh Hiv¥cni din surse deschise (cum ar fi publicaţiile militare), Imlimmi,

iiic furnizate în cadrul contactelor stabilite de ataşaţi sau îi... im.i (şi cu reprezentanţi militari ai statelor considerate adversare, rherca (fie directă, fie prin intermediul mijloacelor tehnice ihm în a desfăşurărilor de forţe sau ale exerciţiilor militare ori mm* umane cu acces direct la planuri militare. În ceea ce priveşte imlhmii.i (iiic ştiinţifice şi tehnice, această categorie de analiză necesită

Mâinii, iica prognozei informative (în care se concentrează toate ini Miii Mtiile despre adversar şi care ilustrează concepţia militară a

Milita) cu cea analizată de specialiştii militari (ce concentrează l»t unea capacităţii militare şi forma în care se va manifesta

4Immiil prognozat).

%Mi laliştii militari trebuie să dea dovadă de flexibilitate în gândire Ume i *i.*md emit aceste prognoze în scopul depistării diferitelor soluţii r... luadversarul le-ar putea adopta în cazul problemelor militare

Mţniiic, soluţii ce derivă din resursele pe care le deţin. Pe scurt, ilinirgii au nevoie de informaţii referitoare la *diversitatea*

*Hf-loftiilor militare* – informaţii care să dezvăluie metodele de I«iure ale inamicului, conflictele interne şi modul cum acţionează, I»! în nu şi aspectele conceptuale divergente" 35.

I hi exemplu în acest sens este oferit de către francezi referitor la i-i.în de luptă germane de la începutul Primului Război Mondial, dimrgia germană (Planul Schlieffen) era de a evita un atac direct iMiţioinva Franţei, prin efectuarea unor operaţiuni militare în Belgia. h... în fost urmate de

desfăşurări de trupe de-a lungul graniţei îi mm o pelgiene. Totuşi, pentru a pune în aplicare acest plan, a fost h vonca germanii să arunce rezerviştii în luptele din linia întâi; în

1/11 mii rar, nu ar fi avut destui oameni pentru teatrul de operaţiuni

«im* se desfăşura pe flancul belgian şi pentru poziţiile defensive de-a hiiiK.-ul graniţei franco-germane. Comandanţii francezi deţineau informau cu privire la planurile Germaniei pe care le-au subestimat, în ulerându-le nerealiste: ei au refuzat să creadă că omologii lor 111 m.mi-ar trimite în linia întâi rezerviştii din moment ce ei înşişi nu în li făcut acest lucru. Astfel, francezii au interpretat greşit locul în m în vor ataca germanii – nu din cauza lipsei informaţiilor, ci fiindcă ini, ui vrut să înţeleagă faptul că armata germană ar putea opera altfel»şi. Îl ei.

În cele din urmă, când operaţiunile militare sunt iminente sau chiar încep să se desfăşoare, trebuie să existe informaţii cu privire U dispozitivele militare şi la deplasarea forţelor. Acest tip de informait! reprezintă datele primare pentru ceea ce cunoaştem sub numelo „indicaţii şi avertizări", care se referă la evitarea surprizelor strategice.

*Informaţii politice*. Acestea sunt informaţii care privesc proceselo politice, ideile şi intenţiile ţărilor străine, facţiuni şi lideri. Analiza acestor informaţii este similară cu a celor provenite din surse academice şi jurnalistice, precum şi din comentariile cu privire la politica internă şi internaţională a altor state. O diferenţă evident!

constă în existenţa surselor secrete, umane sau tehnice (în principal informaţiile din comunicaţii), care furnizează informaţii ce nu sunt disponibile pentru comentatorii publici.

Importanţa acestor surse suplimentare depinde de natura regimului ţării studiate, precum şi de numărul şi calitatea surselor de informaţii despre ţara respectivă. Cu cât o ţară este mai democratică şi mal deschisă, cu atât este mai uşor de studiat viaţa sa politică, fără a face apel la sursele de informaţii. În mod contrar, în ţările în care deciziile politice esenţiale sunt luate de către indivizi (ori familii sau partide), sursele de informaţii devin mai importante şi mai greu de obţinut. Totuşi, chiar şi în cazul unei societăţi închise, pot exista informaţii din surse deschise care, dacă sunt analizate cum trebuie, dezvăluie mult mai multe lucruri despre viaţa politică decât la primă lectură. De exemplu, după cum am menţionat în cazul culegerii de informaţii din surse deschise, informaţiile biografice (cum ar fi faptul că A pare să-i fie recunoscător lui B pentru promovările sale anterioare) despre liderii unei ţări pot fi analizate pentru a avea o imagine despre luptele interne; chiar şi într-un regim ce afişează public o imagine de unitate se pot deduce luptele interne prin observarea modului în care şi-au obţinut poziţiile protejaţii liderului.

În plus faţă de problema disponibilităţii unor surse de informaţii secrete, o diferenţă importantă între analiza informaţiilor provenite din sfera politică şi activitatea academică sau jurnalistică este modul de lucru. Analiştii trebuie să ofere

răspunsuri oportune. Munca lor este inutilă dacă rezultatele nu ajung la factorii decizionali înainte ca aceştia să fie forţaţi de circumstanţe să acţioneze. Dimpotrivă, cercetătorii au timpul de partea lor. În plus, ei lucrează singuri, ifeg AIM lti şi singuri temele; ofiţerii analişti execută ordine şi lucrează Im în hipll l niiţinuiul analizelor efectuate de ofiţerii analişti în comparaţie fH iele de cercetătorilor este determinat de scopul şi de modul în... r desfăşoară aceste activităţi. Ofiţerii analişti urmăresc să» MHI/1 în evidenţă acele aspecte care interesează factorul politic; Mi imaioi îi urmăresc în mod special doar acele aspecte pe care ei le h h îi t fi cele mai importante. Acest aspect este discutat pe larg în»j«şi”! iil o, referitor la relaţia dintre informaţii şi politică.

*Informaţii economice şi sociale*. Acestea se referă la aceleaşi tu în nene care fac obiectul de activitate al ştiinţelor sociale cel puţin im!«i.iii.i în care ele interferează cu problemele cotidiene importante. Intui mnţiile politice se concentrează asupra acelor informaţii cerute 1* fut lorii politici. Activitatea de analizare a acestor informaţii este de niullc ori socotită a fi mai puţin complexă – atât în teorie, cât şi Im pim Lică – decât studiile academice în ciuda faptului că nu apar lutriniţe substanţiale în modul de lucru.

Nu doar că metodele cercetării academice şi ale celor efectuate **» specialiştii militari sunt în mare măsură aceleaşi, ci şi specialiştii i *mv* lucrează în aceste domenii sunt puşi în faţa aceloraşi probleme „— Mi când efectuează evaluări ale informaţiilor, din moment ce Ihm în

puţine sunt obţinute prin metode secrete. Aşadar, o estimare»În mată de către un analist de informaţii cu privire la viitorul unei şi nu va diferi prea mult de cea a unui cercetător sau a unui grup h experţi dintr-o universitate. Cu toate acestea, uneori este nevoie «H *se* aplice metodele de obţinere a informaţiilor secrete. Multe Iniinmaţii economice despre fosta Uniune Sovietică au fost ţinute în i iele, printre acestea şi cele referitoare la rezervele de aur, precum şi l, i vânzările anuale de aur pe piaţa internaţională. În timp ce un iilliri de informaţii este deseori forţat să estimeze aceste cifre în o «l.îşi fel în care ar face-o un economist, o sursă de informaţii poate nu ni/.a indicii sau chiar cifrele oficiale sovietice. Totuşi, contribuţia m.clor de informaţii la analiza economică şi socială este redusă.

Agenţiile de informaţii nu pot să-i atragă cei mai buni analişti în iliutieuiu. Libertatea vieţii academice se dovedeşte a fi mai atractivă lui turn specialiştii talentaţi din domeniul ştiinţelor sociale, chiar dacă liniile sunt mai mici. În plus, companiile multinaţionale, băncile şi firmele de brokeraj pot supralicita cu uşurinţă agenţiile de informai!) în ceea ce priveşte salariile oferite economiştilor calificaţi. Nu exialt niciun argument care să justifice faptul că analizele efectuate de către analiştii de informaţii în problemele economice, care nu implicH societăţile ce ţin secrete bazele lor de date, să fie superioare celor făcute de către economiştii din lumea afacerilor37. Bineînţeles e analiza economică efectuată în lumea afacerilor este considerată o

informaţie cu drepturi de autor şi nu e la dispoziţia factorilor decizionali din guvern, dar măcar o parte din ea ar putea fi, prin intermediul serviciilor de consultanţă sau a buletinelor de afaceri.

Produsul activităţii serviciilor de informaţii

Produsul activităţii serviciilor de informaţii este reprezentat de orice mijloc, de la un raport oficial la o scurtă conversaţie, prin care un analist de informaţii transmite date prelucrate factorilor de decizie sau comandanţilor militari ce au nevoie de ele şi le pot utiliza. În secţiunea de faţă sunt analizate diferitele forme pe care le poate lua produsul activităţii de informaţii şi utilitatea acestora. Clasificarea are un caracter general, iar terminologia este cea utilizată în mod obişnuit de agenţiile de informaţii americane, fără a exista însă una standard.

În general, produsele activităţii serviciilor de informaţii sunt împărţite în trei categorii: *informaţii curente*, *informaţii de bază* şi *estimări informative*. Această clasificare corespunde modelului propus de Sherman Kent; într-o terminologie proprie, acesta menţionează „forma curentă caracteristică reporterilor" a informaţiilor, „forma descriptivă de bază" şi „forma speculativ-estimativă", arătând că acestea vizează informaţiile referitoare la prezent, trecut şi, respectiv, viitor38. Pentru ilustrarea diferitelor tipuri de produse ale activităţii de informaţii am utilizat, în principal, exemple din SUA, deoarece în cazul acestora am avut la dispoziţie informaţii mai detaliate decât pentru alte ţări. Distincţiile au însă

aplicabilitate generală, chiar dacă accentul pus pe diferite produse variază de la un serviciu de informaţii la altul.

Miniminţiile curente ţfrtiţiilor de informaţii au diverse produse menite să aducă la cunoşineh (miorilor de decizie noile date de interes deosebit care pot tăftu Milii politicile adoptate. În această privinţă, agenţiile au un rol Hmt Mi relui îndeplinit de presă39. Sfera informaţiilor depinde de ihhm în lr naţionale. Evident, trebuie stabilite anumite priorităţi, în fim* *w* de ceea ce este, potrivit lui Kent, „relevant pentru problemele FMIM iiutr curente şi alte probleme care se întrevăd” 40. Chiar dacă H HII un sistem de priorităţi, la acesta trebuie să se adauge evaluările 1». lui Iuţilor din serviciile de informaţii cu privire la aspectele care ßtüftnlă importanţă pentru utilizatori. Aceste evaluări depind, la Uimii lor, nu numai de perspicacitatea analiştilor de informaţii, ci şi.1* imensiiatea interacţiunii lor cu factorii de decizie.

Iu Statele Unite, cel mai cunoscut produs de acest gen este *hhuimirea zilnică a preşedintelui* (*President’s Daily Brief* – PDB). \» «-linia trebuie să includă „informaţii de cea mai mare importanţă, în Mini e preşedintelui pentru îndeplinirea responsabilităţilor pe linie»lr mm utilate naţională” şi le „este transmisă doar preşedintelui, Mi ppieşedintelui şi unui grup restrâns de oficiali din cadrul executivului, desemnaţi de preşedinte” 41. Potrivit aprecierilor făcute în l wu de Cord Meyer, un fost oficial CIA:

I ale conceută astfel încât să poată fi citită

de preşedinte în 10 – 15 minute, la începutul fiecărei zile de lucru. Nu se doreşte a fi o recalculare a evenimentelor relatate de mass-media în decursul ultimelor i tic ore, ci o scurtă prezentare a semnificaţiei celor relatate de sursele mm rele în legătură cu evoluţiile curente de pe plan mondial42.

*Informarea principalilor factori de decizie* (*Senior Executives Iniftlixence Brief* – SEIB), care a înlocuit un document anterior, ni a mi *Raportul informativ zilnic* (*National Intelligence Daily* – NID), Mir distribuit pe scară mai largă. SEIB este „alcătuită în baza MIH sultărilor cu alte agenţii de informaţii" şi include „informaţii uimie esenţiale[,] ... prezentate astfel încât să răspundă cerinţelor Hht lalilor de rang înalt din cadrul guvernului Statelor Unite, cu ninhutii în domeniul asigurării securităţii naţionale" 43.

Din când în când se face auzită opinia potrivit căreia agenllllf de informaţii ale Statelor Unite dedică prea mult timp şi efort pentru îndeplinirea acestei atribuţii de „informare curentă", ceea ce f afectează capacitatea de a analiza în profunzime diverse situaţii. D exemplu, într-un raport al unei comisii senatoriale privind depui! tamentul de analiză al CIA, Direcţia de Informaţii (DI), s-o facem, următoarele comentarii, sub titlul „Sindromul evenimentelor curente»H

Sarcina de a realiza rapoarte informative curente – care analizen/i evenimentele zilnice în vederea unei informări rapide – consumă!» prezent prea multe resurse din cadrul DI. Răspunzând cererilor sport (de informaţii de

interes imediat venite din partea factorilor de deciziţ de abordare pe larg a mai multor subiecte, DI a fost nevoită să recurg în mare parte a activităţii sale de cercetare, la o abordare axată * „evenimentele curente”. Analiza aprofundată a problemelor cu impofţtanţă pe termen lung pentru factorii de decizie prezintă mai puţin interj şi s-a alocat un volum mai mic de resurse în acest scop... Potrivit unor observatori, acest sindrom a avut un impact negativ asupf nivelului calitativ al avertizărilor cu privire la posibile crize şi asupri identificării tendinţelor pe termen lung. Abordarea axată pe „eveniment curente” a condus la problema „analizei incrementale” – tendinţa d concentrare asupra celei mai recente informaţii, fără a lua în calcul, în mod sistematic, ansamblul de date integrate acumulate în timp. Grăbindu-H să sistematizeze datele zilnice, analiştii au tendinţa de a pierde clin vedere factorii şi conexiunile ce stau la baza lor”.

Din simplu fapt că această critică a continuat să se facă auzită în decursul anilor se poate trage concluzia că presiunile exercitate în direcţia abordării evenimentelor curente – având la bază dorinU factorilor de decizie de a fi ţinuţi la curent cu ştirile „fierbinţi” – sunt, în mod inerent, puternice şi vor avea deseori câştig de cauză în faţa dorinţei analiştilor de informaţii de a realiza evaluări de mai mare profunzime45. Cu aceleaşi presiuni se confruntă, probabil, şi agenţiile de informaţii din alte ţări.

Semnale şi avertizări

Una dintre cele mai importante funcţii ale

unei agenţii de informaţii este de a avertiza din timp cu privire la eventuale acţiuni militare ostile; în era nucleară, importanţa acestei funcţii este cu atât mai

Mtil Mită De fapt, factorul principal care şi-a pus amprenta asupra hangului sistem de informaţii american postbelic a fost probabil i i n serviciile de informaţii antebelice nu au reuşit să transmită I PŞIII/iue în legătură cu atacul japonez de la Pearl Harbor.

(MIA fiind importanţa sa (în special în perioada Războiului Rece, ilMtl Ninicic Unite, URSS şi aliaţii lor aveau importante forţe armate t nu de arme nucleare care puteau fi îndreptate împotriva adver-fetului) şi întrucât putea fi necesară luarea rapidă a unor decizii, frMftlă Innсţie a agenţiilor de informaţii a fost sistematizată într-o ÜIimia mult mai mare decât oricare alta (cel puţin în Statele Unite). Imhiiul, cunoscut sub numele *semnale şi avertizări* (*Indications ţm-l Wtniings* – I & W), are la bază analizarea demersurilor inevi-liNile urni probabile pe care le-ar întreprinde un adversar în vederea fMfgfith îi unui atac armat. Aceste evenimente ipotetice – mobilizarea iMH vililor, poziţionarea avansată a forţelor militare, schimbarea făihtli Mci de comunicare şi aşa mai departe – poartă numele de

Mnllt valori”; atunci când evenimentul se produce şi este observat, numit „semnal”. Analiştii stabilesc gravitatea ameninţării în *hm*lie de ansamblul semnalelor şi emit avertizări de diferite niveluri”.

Hejj (îordievski, un ofiţer KGB care a desfăşurat activităţi de ijunnai pentru serviciile britanice de informaţii între anii 1975 şi uev a dezvăluit o serie de proceduri I & W utilizate de fosta I Itiiinr Sovietică. Potrivit acestuia, în 1981 Politbüro a ordonat KGB şi uiviciului de Informaţii Militare (GRU, conform iniţialelor lumii) să colaboreze în vederea realizării unui nou sistem de Humiioi i/are la scară mondială, astfel încât să poată fi sesizate îmi!» iile unui posibil atac nuclear occidental. GRU răspundea de Mimuluiizarea indicatorilor strict militari, în timp ce KGB avea în mm mă urmărirea indiciilor care să ducă la luarea unei decizii politice lansare a unui atac nuclear. Printre indicatorii pe care trebuia sa cu iiituiiiorizeze sediul KGB din Marea Britanie se numărau:

pioramul activităţilor de pe Downing Street 10 (reşedinţa primii unistrului), Ministerul Apărării, Ministerul de Externe, Ambasada Statelor Unite şi sediile centrale ale serviciilor britanice de informat îi şi securitate (de exemplu, erau luminile aprinse noaptea?); liecvenţa cu care se deplasau curierii între aceste instituţii; nsirile şi plecările premierului şi ale altor miniştri importanţi ttir exemplu, făcea premierul mai multe vizite la Palatul Buckingham decât în mod obişnuit?); existenţa unor măsuri neobişnuite de apărare civilă, cum ar fi constituirea unor rezerve de alimente sau pregătirea unor bănci de sânge pentru situaţii excepţionale.

Rapoartele de rutină urmau să fie elaborate din două în două sân* tamâni, dar orice

evenimente ieşite din comun trebuiau raportate imediar.

Un astfel de sistem formalizat, în care indicatorii sunt stabiliţi în prealabil şi pot orienta într-o anumită măsură procesul de culegere I informaţiilor, garantează faptul că ele nu sunt ignorate, ci incluse în procesul de elaborare a politicilor. Acest lucru este însă valabil dom în cazul problemelor de importanţă deosebită, cum ar fi o posibili acţiune militară ostilă. În alte privinţe nu există, de regulă, un sistei automat care să garanteze luarea în calcul a informaţiilor disponibil în procesul decizional.

După ce CIA a fost considerată în mare măsură răspunzătoare dl faptul că nu a existat o avertizare cu privire la revoluţia iraniană dil 1978 – 1979, s-au avansat propuneri de creare a unui sistem politic d I & W, pentru a avertiza în legătură situaţiile de instabilitate politic din alte ţări. Aceasta ar presupune stabilirea unor indicatori similar celor utilizaţi în cazul avertizărilor referitoare la eventuale atacuri militare. Acest lucru este mult mai dificil de realizat în domeniul politic comparativ cu cel militar, aşa cum a demonstrat-o, o dată în plus, prăbuşirea rapidă şi neaşteptată a regimurilor comuniste difl Europa de Est, în 1989, şi din Uniunea Sovietică, în 1991; eşti puţin probabil ca stadiul actual al ştiinţelor sociale să permitl obţinerea unor rezultate suficient de credibile, astfel încât să aibă o utilitate reală. Cu toate acestea, un sistem mai riguros ar clarifici responsabilităţile ce revin agenţiilor de informaţii

în ceea ce priveşte transmiterea unor avertizări cu privire la posibile evenimente grave, chiar şi atunci când factorii de decizie nu îşi concentrează atenţia asupra respectivei ţări sau regiuni.

Informaţiile de bază

O altă categorie generală de produse ale activităţii serviciilor de informaţii este „raportul informativ de bază”. Un astfel de raport încearcă să ofere o imagine cât mai completă a unei anumite situaţii, valorificând atât date din surse deschise, cât şi informaţii relevante ittyliiule din toate sursele secrete disponibile. De exemplu, în domeniul militat, un produs de acest gen se poate referi la dispozitivul de iuj»în mod asemănător, un raport informativ de bază privind înlemni politic al unei ţări poate include o trecere în revistă a tuturor Mlrlor şi personalităţilor politice importante, a viziunilor lor Mfulltionale, a legăturilor dintre ele şi aşa mai departe.

Nttpoartele periodice

Ihipă cum I & W reprezintă o formă sistematizată a informaţiilor în rute referitoare la o anumită problemă de mare importanţă, pot în Inia serii speciale de rapoarte care abordează anumite probleme. Iu exemplu, în perioada Războiului Rece, serviciile americane de Inf oimaţii au realizat rapoarte semestriale referitoare la modul în unr sovieticii respectau acordurile privind armele nucleare Stralau e; aceste rapoarte conţin cele mai solide evaluări în legătură cu Ionele nucleare strategice ale ţării respective, cu relevanţă pentru Mulurile în cauză. În 2001, Direcţia de Informaţii a CIA (DI) a im/cutat pe site-

ul său următoarea listă de rapoarte periodice:

*Regional Reviews*. Evaluări periodice (începând de la unele cu frecvenţă zilnică până la cele lunare) ale problemelor politice, economice, militare şi sociale din alte ţări, cu relevanţă pentru interesele Statelor Unite… care abordează evenimente regionale şi naţionale din Africa, Europa, America Latină, Orientul Mijlociu, Asia, precum şi statele slave şi euroasiatice din fosta Uniune Sovietică;

*The Terrorism Review*. Un raport lunar, care analizează tendinţele actuale ale terorismului internaţional şi metodele utilizate… inclusiv o cronologie a incidentelor teroriste ce au avut loc pe plan internaţional;

*The Narcotics Monitor*, care analizează evoluţiile înregistrate pe plan mondial în domeniul narcoticelor;

*Proliferation Digest*, ce apare lunar şi cuprinde articole pe teme de proliferare;

*The International Arms Trade Report*, cu apariţie bilunară.

K.ipoartele informative cu evoluţii de perspectivă i va mai ambiţioasă categorie de produse ale activităţii serviciilor de informaţii este aceea care nu se limitează la descrierea situaţiei actuale, ci încearcă să anticipeze modul în care va evolua ea. În limbajul serviciilor americane de informaţii, astfel de lucrări sunt numite estimări. Un loc aparte îl ocupă *estimarea naţională di securitate* (Na*tional intelligence estimate* – NIE), ce reprezintă cea mai competentă evaluare cu privire la un anumit subiect a comunităţii

agenţiilor americane de informaţii.

Aceste estimări sunt menite să ofere cea mai amplă viziune asupra subiectului în cauză şi să proiecteze situaţia actuală în viitor. În Statele Unite, ele sunt realizate de un personal special desemnat, cu sprijinul analiştilor din toate agenţiile de informaţii. Estimările includ punctele de vedere ale tuturor agenţiilor din cadrul comunităţii de informaţii48. Se depun mari eforturi pentru a se ajunge la un consens, dar, atunci când acest lucru nu este posibil, se poate exprima o opinie diferită într-o „notă de subsol”, deşi uneori ea este inclusă în text.

NIE cu privire la anumite subiecte de importanţă deosebită sunt elaborate anual (sau la alte intervale regulate de timp); alte subiecte sunt analizate în urma unor solicitări precise, venite fie din interiorul comunităţii de informaţii, fie de la alte organisme guvernamentale, cel mai frecvent de la National Security Council (NSE). În urma unor solicitări urgente, pot fi elaborate estimări mai concise, referitoare la subiecte de interes imediat, cunoscute sub denumirea NIE speciale (sau SNIE).

Spre deosebire de practica americană, în Israel, înainte de Războiul de Yom Kippur din 1973, estimările erau realizate exclusiv de direcţia de informaţii militare, un departament din cadrul armatei. Deşi existau şi alte servicii de informaţii – Institutul Central pentru Informaţii şi Securitate (Ha-Mossad), care desfăşura operaţiuni secrete în alte ţări, Shin Beth, ce răspundea de contrainformaţii şi antiterorism, şi departamentul

de cercetări al Ministerului de Externe –, doar Direcţia de Informaţii Militare avea acces la toate datele şi răspundea de analizarea şi transmiterea acestora. Mai mult, membrii Cabinetului nu aveau experienţă în activitatea de informaţii şi nu exista vreun mecanism prin care conducerea politică să ordone Direcţiei de Informaţii Militare să furnizeze evaluări pe anumite teme. Această concentrare a puterii a fost criticată ulterior, considerându-se că a contribuit la eşecul serviciilor israeliene de informaţii, care nu au anticipat atacul egipteano-sirian din 6 octombrie 1973 ittililtM! analizat în secţiunea „Eşecurile serviciilor de informaţii şi Mtftimi iuefe nepravazute” din acest capitol) 49.

Diferenţieri între serviciile de informaţii l»ul funcţiile legate de informarea curentă şi de bază par a fi Mt iipule pentru activitatea serviciilor de informaţii din orice ţară, în îi infisură se regăseşte însă funcţia estimativă în activitatea lor? iMipoiunţa acesteia diferă de la o ţară la alta şi de la o perioadă la în I) e exemplu, în Statele Unite, elaborarea estimărilor este consilhuM forma supremă a activităţii serviciilor de informaţii. În schimb, în Uniunea Sovietică, în anii ’30, Stalin dorea să deţină controlul năupui funcţiei estimative; el a ordonat NKVD (precursor al KGB) «a nu îi trimită estimări sau evaluări ale situaţiei externe, ci să se ihul Uve la raportarea informaţiilor secrete (rapoarte primite de la htim maiori de rang înalt) pe care le obţinea50. Acest subiect vizează h lupa dintre funcţia de informare şi cea decizională din cadrul unui guvein, aspect

analizat în capitolul 6.

(cocurile serviciilor de informaţii l evenimentele neprevăzute lipuri de eşecuri

*Mtu ul-surpriză*. Riscul ca serviciile de informaţii să nu evalueze

«în ci i o situaţie a existat dintotdeauna în activitatea lor. În secţiunea»! hiţâi sunt analizate acele cauze ale eşecurilor care ţin de propriul»până (de informaţii; în capitolul 5 va fi analizat modul în care i, nul poate fi determinat de strategiile de inducere în eroare aplicate un adversar.

I {secul cel mai grav şi care se poate solda cu cele mai mari pirjudicii se înregistrează atunci când are loc un atac neanticipat şi lui (ele militare ale ţării sunt luate prin surprindere. Într-adevăr, aşa unsa arătat deja, configuraţia actuală a comunităţii americane de minunaţii se datorează în mare măsură eforturilor de remediere a li l menţelor ce au condus la situaţia în care ţara a fost luată prin surprindere de atacul japonez de la Pearl Harbor, din 7 decembili 1941.

Există numeroase lucrări care au ca subiect atacurile-surpriză reuşite. Atacarea Uniunii Sovietice de către Germania la data de 22 iunie 1941 şi atacul egipteano-sirian asupra Israelului din 1973 (care a declanşat Războiul de Yom Kippur) se numără, alături de atacul de la Pearl Harbor, printre cazurile analizate cele mai frecvent51, Chiar şi în timpul unui război, când este de presupus că forţele militare sunt într-o stare de mai mare alertă decât în timp de pace, se pot produce surprize de proporţii. Exemple în

acest sens sunt atacul german din Ardeni, din decembrie 1944 (bătălia de la Bulge), intrarea Chinei în războiul coreean din noiembrie – decembrie 1950 şi ofensiva nord-vietnameză şi a Vietcong-ului (ofensiva Tet) asupra „Vietnamului de Sud la sfârşitul lunii ianuarie 196852.

Foarte asemănătoare cu neanticiparea unui atac este situaţia când o ţară se aşteaptă la un atac, dar, din cauza unor estimări eronate cu privire la locul şi modul în care va avea loc acesta, reacţionează inadecvat. Un exemplu concludent în acest sens este reacţia Germaniei la debarcarea Aliaţilor în Normandia, la data de 6 iunie 1944 (Ziua Z). Germanii se aşteptau, în mod cert, la un atac, dar erau atât de siguri că acesta va viza regiunea Pas-de-Calais, încât au considerat că Normandia este o diversiune şi au ratat o bună ocazie de a contraataca în forţă atunci când capetele de pod erau cel mai vulnerabile53.

*Alte evenimente neprevăzute*. Deşi un atac neanticipat poate fi evenimentul neprevăzut care afectează cel mai mult o naţiune, el nu este singurul de acest gen. De exemplu, un eveniment politic neaşteptat (cum ar fi o schimbare a alianţelor sau o lovitură de stat prin care este înlăturat un conducător cu care existau relaţii de bună colaborare) poate constitui o lovitură serioasă la adresa intereselor de politică externă ale unei ţări. Modul în care americanii au subestimat, în 1978, problemele politice cu care se confrunta şahul Iranului şi amploarea opoziţiei faţă de regimul acestuia reprezintă unul dintre cele mai cunoscute exemple de eşecuri de acest

gen înregistrate în activitatea serviciilor de informaţii54.

În mod asemănător, absenţa avertizărilor cu privire la o schimbare economică majoră şi rapidă, aşa cum s-a întâmplat atunci când agenţiile de informaţii americane nu au anticipat „şocul petrolului” it Mi I i / l o creştere rapidă a preţului petrolului pe plan mondial –, itofittr li catalogată, de asemenea, drept un eşec al activităţii serii» Mloi de informaţii, în funcţie de ceea ce se consideră că intră în lor tic responsabilitate. Aşa cum s-a arătat, rolul activităţii Ut vii Îilor de informaţii în privinţa problematicii economice este hmi Imprecis şi mai complicat decât în cazul chestiunilor politice sau Hiilihiic în orice caz, criza petrolului din 1973 este un exemplu care nvuionsirează complexitatea acestui tip de probleme, deoarece» «turle fundamentale erau de natură economică (preţul scăzut al tumulului de până atunci a încurajat consumul şi a descurajat acti-Miaiiiv de prospectare şi dezvoltare), în timp ce cauza imediată era Mi» «politică (sprijinul acordat de ţările arabe furnizoare de petrol

I pipiului şi Siriei în Războiul de Yom Kippur din octombrie 1973) 55.

I»ara dezastrele care pot rezulta în urma confruntării cu atacurim pl. t/;1 pe câmpul de luptă sunt evidente, prejudiciile provocate de mi anticiparea unor evenimente politice sau economice sunt mai greu 1» evaluat. În mare măsură, acestea depind de măsura în care tio n nul ar fi fost pregătit să ia măsuri, dacă ar fi fost avertizat şi de i-i IMenta unor strategii ce ar fi

putut să evite producerea evenimentului sau să diminueze impactul său negativ.

se exemplu, nu este clar ce acţiuni ar fi întreprins Guvernul Ciulelor Unite dacă ar fi fost avertizat în legătură cu şocul petrolului ihn *l*) *73*. În mod similar, evaluarea corectă a problemelor politice ah şahului ar fi fost cu totul altceva decât stabilirea măsurilor care 4 ui li putut lua în privinţa acestora; succesul primului demers nu ar

Îl *y*, îi antat, obligatoriu, şi succesul celui de-al doilea.

*Alte tipuri de eşecuri*. Cele mai multe dintre eşecurile înregistrate în activitatea serviciilor de informaţii presupun, mai devreme sau mai târziu, un eveniment surprinzător, dat fiind că o viziune eronată în upi a lumii înconjurătoare va conduce la un moment dat, într-un fel, au altul, la apariţia unei situaţii nefavorabile neprevăzute. (Există însă. Şi cazuri în care, în urma unei activităţi deficitare a serviciilor. În informaţii, o armată sau o ţară, care nu este conştientă de v uluerabilitatea unui adversar, nu a profitat de o situaţie favorabilă56. În situaţii de acest gen este vorba de un eşec, dar nu de o „surpriză”) Iu orice caz, noţiunea de *surpriză* nu este probabil cea mai utilă pentru înţelegerea prejudiciilor pe care le pot provoca eşecurile serviciilor de informaţii.

Un eşec în activitatea serviciilor de informaţii constă, în esenţi, în înţelegerea incorectă a unei situaţii, fapt ce determină un guvern (sau forţele sale militare) să întreprindă acţiuni inadecvate sau contra-productive din perspectiva intereselor sale. Faptul că este luat prin surprindere de ceea ce se

întâmplă e mai puţin important decât el acţionează sau continuă să acţioneze într-o manieră greşită. Astfel, eşecul activităţii serviciilor germane de informaţii în ceea ce priveşti debarcarea din Normandia din Ziua Z nu a constat atât în faptul el Armata germană a fost luată prin surprindere, cât în evaluarea greşiţi a debarcării din Normandia, considerând-o o diversiune menită st distragă atenţia de la invazia „reală”, care ar fi vizat regiunea Pas de – Calais57. În mod similar, principala cauză a înfrângerii forţelor ONU în Coreea de către chinezi, în decembrie 1950, a fost mal degrabă o înţelegere fundamental greşită a doctrinei şi tacticilor Chinei decât o „surpriză” 58.

În plus, evenimente surprinzătoare care implică neanticiparea acţiunilor unei forţe ostile sau a şanselor de reuşită sunt consemnate, în special, în cazul ţărilor aflate în defensivă, din punct de vedere strategic sau tactic. Dar şi o naţiune aflată în ofensivă poate avea de suferit din cauza estimării eronate a efectivelor adversarului sau a altui factor relevant. De exemplu, atacul Aliaţilor asupra podului de la Arnhem, Olanda – „podul prea îndepărtat” –, din septembrie 1944 a eşuat, în principal, din cauză că, în condiţiile unei prea mari încrederi în forţele proprii şi analizei superficiale a datelor disponibile, responsabilii cu activitatea de informaţii nu şi-au dat seama că în imediata apropiere se aflau două divizii germane de blindate59.

În cele din urmă, eşecurile analizate anterior implică o interpretare greşită care iese la iveală

rapid după ce una dintre părţi trece la acţiune. Alte eşecuri presupun estimarea incorectă a unui proces sau a unei situaţii de durată, caz în care, dat fiind că nu se întâmplă nimic care să demonstreze situaţia reală, este posibil ca eroarea să persiste un timp mai îndelungat. De exemplu, comunitatea americană de informaţii a făcut atât supraestimări, cât şi subestimări ale arsenalului strategic al fostei Uniuni Sovietice, acestea punându-şi ani de zile amprenta asupra viziunilor strategice ale Statelor Unite. Cele

MMI i iinoscute dintre aceste erori sunt poate supraestimările de pupoiţii referitoare la armamentul strategic al sovieticilor, care o mi Indus americanilor senzaţia că au rămas în urmă în ceea ce tviilic numărul bombardierelor, la jumătatea anilor ’50, şi în ceea ce priveşte numărul de rachete, începând cu sfârşitul anilor ’50 şi n4 u/1 lu’ I96160. Dar cel puţin la fel de importantă a fost şi tendinţa, Hmuilesiaia de la jumătatea anilor ’60 şi până la începutul anilor ’70, în subestima ritmul în care Uniunea Sovietică îşi consolida forţele tu medice61.

I.mi/ole eşecurilor

— Îi excepţia cazurilor în care nu pot fi obţinute niciun fel de minimaţii relevante, eşecurile din activitatea de informaţii sunt legate uv o dereglare a procesului analitic, ce determină ignorarea sau Nun pictarea greşită a datelor. Prin urmare, ele sunt similare erorilor înm îl ice oricărui demers intelectual – de exemplu, o greşeală făcută în un istoric în interpretarea unui text foarte vechi, care conduce la iU în ucrea

incorectă a unui aspect al Antichităţii, sau o greşeală a unui nicleorolog în ceea ce priveşte evaluarea importanţei unui sistem ilt presiune scăzută, ce conduce la o prognoză incorectă cu privire la unim vremii din ziua următoare.

Iu plus, anumite particularităţi ale procesului de analiză a Informaţiilor pot determina şi alte eventuale erori. Deşi analiza Informaţiilor este o activitate intelectuală, ea se desfăşoară, spre în îşi bire de activitatea unui om de ştiinţă, într-un cadru instituţional, i în conformitate cu anumite proceduri standardizate, astfel încât n /uliului final este mai degrabă produsul unui sistem decât al unei im isoane. Ca atare, analiza informaţiilor este expusă anumitor pro – ilnne instituţionale specifice. În această secţiune sunt abordate unele la îi ic cauzele eşecurilor înregistrate în activitatea serviciilor de informaţii, fiind analizate mai întâi cele de ordin instituţional, iar apoi cele care ţin mai mult de componenta intelectuală a activităţii în formaţii.

*Subordonarea activităţii de informaţii faţă de factorul politic*.

«.m/.a cea mai discutată a erorilor sau a subiectivismului din analiza mie irmaţiilor este probabil legată de posibilitatea ca evaluările informative să fie făcute astfel încât conducă la rezultatele dorite de superiori, l nu la cele indicate de datele existente. Aceasta este însă o cauză din afara procesului de analiză propriu-zis (presupunând că analistul îl dă seama că aprecierile formulate vin în contradicţie cu concluziile sale reale). În consecinţă, este vorba

de o problemă ce ţine de managementul activităţii de informaţii – maniera în care se rapor»tează serviciile de informaţiile la factorii de decizie pe care îi deservesc; acest subiect este abordat în capitolul 6, unde está analizată relaţia dintre activitatea serviciilor de informaţii şi politici.

*Indisponibilitatea informaţiilor la locul şi în momentul în cart sunt necesare*. Date fiind dimensiunile mari ale organizaţiilor implle cate în culegerea şi analizarea informaţiilor, o posibilă sursă I problemelor o constituie faptul că datele din sistem nu le suni accesibile celor care au nevoie de ele la un moment dat. Aceastl indisponibilitate are diferite cauze: de exemplu, normele de securitate care limitează circulaţia informaţiilor secrete, luptele pentru putea dintre instituţii, în cadrul cărora controlul asupra datelor se transformă într-o armă, sau simplul fapt că biroul ce deţine datele nu este la curent cu necesităţile informaţionale ale altui birou62.

În mod similar, pot apărea probleme dacă niciun birou central nu are atât responsabilitatea realizării unor analize într-un anumit domeniu, cât şi acces la toate informaţiile relevante. În cazul în care diferitele aspecte ale unei probleme intră în atribuţiile unor birouri diferite, este posibil ca o informaţie esenţială să fie ignorată dacă semnificaţia ei nu poate fi înţeleasă decât în contextul tuturor datelor disponibile.

Eşecul înregistrat de activitatea serviciilor de informaţii în legătură cu atacul de la Pearl Harbor se explică prin lipsa de comunicare dintre diferitele unităţi operaţionale şi de informaţii

implicate. Cu toate acestea, deşi au existat poate unele probleme de comunicare între conducerea forţelor armate şi cea a forţelor maritime din Hawaii, nu este clar dacă au existat dificultăţi similare între cele două servicii şi la Washington. O problemă mai importantă a fost lipsa unui birou de analiză centralizat, care să dispună de resursele necesare şi să răspundă de evaluarea tuturor informaţiilor relevante, în schimb, se pare că informaţiile erau prelucrate „din zbor" de câteva persoane care lucrau direct pentru anumiţi factori de decizie nivel hialt – fapt ce era o consecinţă a dimensiunii reduse a Imhliiillllor militare americane la vremea respectivă.

*hklh convenţionale*. Succesul oricărui demers intelectual (de mânii»Iu, descoperirile ştiinţifice, dar şi analiza informaţiilor) poate fi i nmpromis de existenţa unor idei convenţionale – opinii despre un «numit subiect care sunt considerate, în general, adevărate, fără a fi Ihm milicicul analizate. Deşi este clar că ele sunt necesare (nu se dedica zilnic mult timp sau efort pentru reanalizarea şi regân-ilui «» iuiuror punctelor de vedere), există riscul ca, pe baza ideilor INwtl Mciuc, să se interpreteze eronat sau să se treacă cu vederea numite date din care reiese că lucrurile stau, de fapt, altfel.

*k* exemplu, în vara anului 1990, opinia vehiculată în rândul «miliţiilor de informaţii şi al diplomaţilor americani era că Irakul nu în invada Kuweitul. Chiar dacă fotografiile realizate din satelit indii nu, la sfârşitul lunii iulie, o concentrare de proporţii a diviziilor.i. Iha ale

armatei irakiene la graniţa kuweitiană, opinia generală hm i n aceasta reprezenta o încercare a lui Saddam Hussein de a-i ini im mă pe liderii kuweitieni, în contextul disputelor privind Mtoducţia şi preţul petrolului, precum şi rambursarea datoriilor Mtfkuim către Kuweit. Această apreciere pornea de la premisa că, în uid i a/boiului abia încheiat cu Iranul (1980 – 1988), Irakul era prea initii pentru a întreprinde o operaţiune militară amplă şi invadarea iniul slut arab de către un altul era, în orice caz, o situaţie nemaiîntâlnită. Dar, la data de 2 august, Irakul a invadat şi a învins Kuweitul63.

I În alt exemplu al modului în care concepţiile convenţionale pot 11 induce la evaluarea incorectă a unui adversar este opinia pe care o aveau britanicii în anii ’30 cu privire la reînarmarea Germaniei, care în nu-i să fie, apreciau ei, limitată ca amploare. Potrivit lui Wesley K. VV.uk în general, [britanicii] se aşteptau ca reînarmarea trupelor germane să icpăşească limitele prevăzute în Tratatul de la Versailles, dar numai pana* la un nivel care să răspundă cerinţelor de securitate naţională. Prin minare, se considera că încălcarea prevederilor de la Versailles nu indica vreo intenţie agresivă… Pe lângă ipoteza generală că obiectivele (ici maniei în materie de reînarmare erau limitate şi aveau un scop defensiv» se considera că ritmul reînarmării urma să respecte principiile de eficienţă. În opinia britanicilor, aceasta însemna că reînarmarea Germani*! va avea loc într-un ritm moderat, în vederea asigurării unor standard» înalte de

profesionalism şi a celei mai bune utilizări a sistemelor de armament. Această viziune tradiţională asupra reînarmării, care demorwtm o înţelegere limitată a dinamicii naziste, a fost poate cea mai însemnai! dintr-o succesiune de subestimări ale capacităţii militare a Germaniei”.

Impactul nefavorabil al ideilor convenţionale asupra raţionamentului individual poate fi amplificat de mediul instituţional în care-l realizează analiza un serviciu de informaţii. Dacă raţionamentul unol persoane poate fi influenţat de existenţa unor date deosebit de claroi care contrazic modelul preexistent, sau chiar de o intuiţie de moment, ce indică necesitatea altei interpretări a datelor, este puţin probabil ca mai multe persoane să fie influenţate simultan în acelaşi fel, Astfel, cei care contestă concepţia convenţională vor întâmpini probabil rezistenţă din partea unui număr mult mai mare de persoane, ce o acceptă în continuare.

Dacă o persoană face economie de timp şi efort prin faptul că nu îşi reanalizează în mod constant toate opiniile, se poate spune că şi o organizaţie procedează în aceeaşi manieră. Având în vedere dimensiunile şi complexitatea organizaţiilor implicate, precum şi necesitatea obţinerii acordului, cel puţin tacit, al unui număr mare de persoane asupra concluziilor la care s-a ajuns, reevaluarea datelor în vederea revizuirii tuturor ipotezelor de bază este un proces foarte dificil şi îndelungat.

Astfel, dacă un analist trebuie să elaboreze un raport, el va studia mai întâi ceea ce s-a scris

în anul anterior şi va face apoi o simplă actualizare. În felul acesta nu numai că nu se mai depun eforturi suplimentare, ci se asigură şi un anumit grad de siguranţă. Întrucât raportul precedent a fost aprobat, în condiţiile în care analistul se limitează la efectuarea modificărilor ce decurg din datele noi, raţionamentul de bază nu mai trebuie repetat şi se reduce la minimum posibilitatea apariţiei unei contradicţii.

Evident, aceasta creează premisele unor erori în cazul situaţiilor care presupun schimbări graduale. Întrucât informaţiile sunt aproape întotdeauna disparate şi incomplete, este posibil ca acumularea unor informaţii noi să nu determine o revizuire a analizei fundamentale. Acest lucru se poate întâmpla chiar şi atunci când majoritatea datelor sugerează că ar fi mai logică utilizarea altui cadru. Există astfel

H-ul, i o viziune învechită asupra unei situaţii să fie menţinută mult m.îi mult decât ar trebui65.

*Vioivetarea unei imagini simetrice*. Cele două aspecte analizate «Minim sunt valabile în primul rând în ceea ce priveşte analiza taftimiaţiilor într-un cadru instituţional. O altă cauză a erorilor NMV căile în procesul de analizare a informaţiilor este însă aplicarea uhu! hiiionament greşit, lucru care se întâmplă într-o mare diversitate *tk* iluut (îi nefiind legat de cadrul instituţional în care se desfăşoară Htdl/II Acest fenomen poate fi denumit „proiectare a unei imagini ihii Pirice”, care presupune că situaţiile nefamiliare sunt interpretate I* lin/.» celor familiare”. În activitatea serviciilor de informaţii», i.» Li înseamnă că

acţiunile altui stat sunt evaluate sau anticipate r im analogie cu acţiunile pe care consideră analistul că le-ar lua el m l-ai a sa) dacă s-ar afla într-o situaţie similară.

De exemplu, faptul că serviciile israeliene de informaţii nu au nullt ipat atacul egipteano-sirian care a declanşat Războiul de Yom i ippur din octombrie 1973 pare să fi fost cauzat, în parte, de acest»muncii; serviciile israeliene de informaţii nu şi-au imaginat că arabii \ i în dei lansa un război pe care, după toate probabilităţile, l-ar fi pierdut67. I» exemplu, cu mai puţin de două luni înainte de izbucnirea războiului, Mimhe Dayan* a afirmat în faţa Statului-Major al forţelor israeliene de npăiare că „raportul de forţe ne este atât de favorabil, încât anulează

«umilerentele arabilor pentru o reluare imediată a ostilităţilor” 68.

I’i ivind însă retrospectiv, se pare că preşedintele Egiptului, Anwar Sadai, a dorit ca războiul să pună capăt impasului în care se găseau h lainic dintre israelieni şi arabi şi nu a mizat, de fapt, pe câştigarea im I»ieşi ulterior a avut loc o răsturnare a situaţiei pe câmpul de luptă, v li am iile iniţiale ale arabilor (în special, traversarea de către egipteni îi «analului Suez şi străpungerea liniilor defensive ale israelienilor) ui asigurat contextul psihologic pentru recâştigarea, în cele din urmă», ivninsulei Sinai. Ignorarea posibilităţii de asumare a unor astfel de i ea un, străină experienţei militare israeliene şi americane, poate în prezenta un exemplu de proiectare a unei imagini simetrice.

Moshe Dayan (1915 – 1981), lider militar şi politic israelian; cel de-al patrulea vet" al Statului-Major al Forţelor de Apărare Israeliene (1953 – 1958) (n.r.).

Un alt exemplu concludent poate fi găsit în raportul Comisiei Chuivh, o comisie specială a Senatului Statelor Unite, înfiinţată în 1975 pentru investigarea comunităţii de informaţii. În raportul respectiv este citai următorul paragraf dintr-un proiect al Estimării Naţionale de Securitul! din 1969, referitor la forţele nucleare ofensive ale Uniunii Sovietico

Credem că sovieticii îşi dau seama de dificultăţile enorme pe care le ni presupune orice încercare de obţinere a unei superiorităţi strategice în măsură să modifice semnificativ echilibrul strategic. În consecinifl considerăm că este foarte puţin probabil ca URSS să încerce, în perioadl vizată de această estimare, să ajungă la capacitatea necesară pentru a dl „prima lovitură", adică pentru a lansa un atac-surpriză împotriva Statelor Unite, fără să înregistreze prejudicii inacceptabile. În mod aproapi sigur, în opinia sovieticilor, costurile unei astfel de operaţiuni, arin rugându-se la costurile aferente tuturor celorlalte operaţiuni militare, ar fi mult prea mari. Mai important este însă faptul că, în mod aproapi cert, ar considera că este imposibil să atingă capacitatea necesară pentru a contracara cu succes diferitele componente ale forţelor strategice dl atac ale Statelor Unite. În cele din urmă, chiar dacă un astfel de proiect ar fi fezabil din punct de vedere economic şi tehnic, sovieticii

ar ajungi aproape cu certitudine la concluzia că Statele Unite îşi vor da seama dl aceste eforturi şi vor întreprinde demersuri similare sau chiar mai ample69.

Lăsând la o parte contextul în care Comisia Church citează acest pasaj (administraţia Nixon şi, în special, secretarul de stat al Apărării, Melvin Laird, sunt criticaţi pentru faptul că au făcut presiuni asupra directorului CIA, Richard Helms, în vederea eliminării acestui pasaj din versiunea finală a NIE, lucru care s-a şi întâmplat), raportul său nu arată dacă evaluările din pasajul respectiv se bazau pe informaţii din interior despre viziunea strategică a Kremlinului. Într-adevăr, din modul de exprimare (de exemplu, „în mod aproape sigur”) reiese că este vorba de opiniile analiştilor în legătură cu viziunea sovieticilor, şi nu de date obţinute direct din documente sau de la informatori de nivel înalt.

Ca atare, este un exemplu de proiectare a unei imagini simetrice, nu numai prin prisma celor trei afirmaţii (ultimele trei fraze) pe care le prezintă în susţinerea ideii sale principale, ci şi prin întreaga manieră de tratare a problemei. Prima afirmaţie conduce la ideea că serviciile americane de informaţii ar fi ştiut ce nivel al costurilor ar

Mhilm iiisiclerat prea mare de către sovietici, apreciere care se baza, în M Itw ipal, pe proiectarea unei imagini simetrice – de fapt Statele Mhh» au ajuns la concluzia că acest obiectiv nu era fezabil din punct 4* hMlete economic. A doua afirmaţie reflectă o idee larg

răspândită fet fdudul strategilor americani, dar care nu era neapărat împărtăşită, momentul respectiv de teoreticienii sovietici din domeniul militar, lu' în le din urmă, cea de-a treia afirmaţie le atribuie sovieticilor o HMune mecanicistă, apolitică asupra cursei înarmărilor (de tipul lM»Hue reacţie), care predomina în Statele Unite, dar nu neapărat şi N» I utunea Sovietică.

VI mai important este poate faptul că modul în care este pusă fMHttlema în primele două fraze – echivalându-se „superioritatea MMietf iefl în măsură să modifice semnificativ echilibrul strategic" cu «pai Halca necesară pentru a da prima lovitură" – reflectă doctrina metit au.1 privind distrugerea reciprocă (*Mutual Assured Destruction* – MAI M. fără a fi făcută vreo încercare de înţelegere a ceea ce i Mi în lei au sovieticii semnificativ la vremea respectivă. Reiese astfel.i» mivieticii ar considera că soluţiile parţiale la problema contra – 4 i«în torţelor strategice ofensive ale Statelor Unite sunt nesemuhi itiive şi nu merită să fie puse în practică.

Dat fiind însă că această opinie este doar implicită, şi nu iipilmată, ea nu este analizată în baza unor date concrete. (De Mrmplu, o evaluare atentă a acestei opinii ar fi trebuit să aibă în bilete accentul pus de sovietici pe apărarea strategică antiaeriană, Mhienţa unor adăposturi subterane pentru membrii conducerii şi «iMemul de apărare împotriva rachetelor balistice de la Moscova, m şi în absenţa unui astfel de sistem la nivel naţional.) Faptul că «rasifi viziune le-a fost atribuită sovieticilor pare să fie un caz de l'iMiiviare a unei

imagini simetrice de către analişti, care considerau» îi logica de la baza viziunii americane era imbatabilă şi, ca atare, h.i împărtăşită şi de sovietici.

O altă formă des întâlnită de proiectare a unei imagini simetrice, i inc afectează capacitatea de evaluare corectă a progreselor ştiinţifice am tehnologice realizate de un adversar în domeniul militar, este a ud romul „aici nu s-a inventat”. Acest sindrom se caracterizează (Hin faptul că nu se ia în serios posibilitatea ca un adversar să fii în ili/al o armă sau un dispozitiv la care propriul sistem tehnico-militar nu s-a gândit sau l-a considerat lipsit de fezabilitate ori de eficienţă.

Acest sindrom se face simţit mai ales atunci când este vorba de in adversar considerat inferior din punct de vedere tehnologic.

R.V. Jones analizează acest fenomen atunci când prezintă activităţi de informaţii desfăşurată de britanici pe linie tehnico-ştiinţifică M perioada celui de-al Doilea Război Mondial. Într-o concluzie formulau pe marginea unui raport informativ privind racheta balistică V-2, care germanii au realizat-o spre sfârşitul războiului şi au lansai «pentru prima dată asupra Londrei la data de 8 septembrie 1944, Jones trece în revistă cele patru posibilităţi legate de o reali/ătf tehnică: în acest caz, britanicii fie reuşesc, fie nu reuşesc, l germanii, la rândul lor, reuşesc sau nu. Sindromul „aici nu i inventat” se materializează atunci când:

…specialiştii noştri fie eşuează, fie nu încearcă, [iar] germanii reuşeu Acesta este cel mai interesant caz din activitatea serviciilor de

informaţii, dar este greu de depăşit prejudecata că, întrucât noi nu am realizat ui lucru, acesta este imposibil sau absurd. În schimb, atunci căné analizează realizarea germanilor, specialiştii noştri se transformă, (f fapt, în novici şi, ca atare, pot emite ipoteze mai hazardate decât cele nil serviciilor de informaţii [adică ale analiştilor de informaţii care nu sui specializti în tehnologia respectivă], care au cel puţin avantajul unul contact mai apropiat cu inamicul70

Soluţia oferită de Jones la această problemă este ca analistul rit informaţii să trateze cu prudenţă opiniile specialiştilor din domeniul tehnic, încercând totodată să valorifice competenţa lor:

Serviciile de informaţii trebuie să se ţină seama întotdeauna de faptul e recomandările vin din partea unui specialist britanic, şi nu german Dacă nu se are în vedere permanent această distincţie, se pot face erori grave. În domeniul militar, Napoleon era perfect conştient de acest risc, făcând referire la „construirea unei imagini a inamicului”. Acelaşi riso există şi în domeniul tehnic71.

„Soluţii” la problema eşecurilor din activitatea serviciilor de informaţii

*Ce este eşecul*? Mai frecvent decât ar fi de aşteptat, având în vedere mitul omniscienţei serviciilor de informaţii, se întâmplă ca

...4M» În sau estimările informative să conţină afirmaţii eronate şi té lot evenimente importante fără ca agenţiile de informaţii să *u* (1 hiiih ipat. Pentru a stabili dacă situaţiile de acest

gen constituie UM nu eşecuri ale activităţii serviciilor de informaţii, este necesar un im!” h Im funcţie de care să fie evaluate performanţele în domeniu72, p HMultleră adesea că activitatea serviciilor de informaţii ar trebui iMliifiin în raport cu un ideal de clarviziune. Se pierde, însă, din & hW i n activitatea de informaţii implică, în general, o confruntare imH i îi un adversar uman, şi nu o luptă metaforică cu natura (aşa unu e întâmplă în cazul cercetării ştiinţifice, care încearcă să febnminc natura să îşi dezvăluie secretele).

I N«exemplu, incapacitatea victimei de a anticipa un atac-surpriză m” le versul succesului repurtat de atacator atunci când îşi surprinde ttvhtwuul. În activitatea serviciilor de informaţii, una dintre părţi lin i ai i îi de cele mai multe ori, să zădărnicească eforturile făcute de»în i nu pentru înţelegerea corectă a situaţiei. În acest scop, aceasta 4 în r uz de o multitudine de tehnici de informaţii, inclusiv de 1” în imuni, după cum se poate vedea în capitolul 5, care abordează lumiiia activităţii de contrainformaţii.

I-i în urinare, progresele înregistrate în privinţa tehnicilor utilizate n» în iivitatea serviciilor de informaţii nu pot fi comparate, de exemelu cu cele din domeniul chimiei. În urma progresului înregistrat.1» en clătile din domeniul chimiei şi a răspândirii noilor rezultatele îi i ne s-a ajuns, chimiştii din întreaga lume pot obţine rezultate mai lume în activitatea lor. În domeniul informaţiilor, lucrurile nu stau în i la Ici; faptul că datele sau procedurile noi permit unui grup de îne

îi de informaţii să obţină rezultate mai bune înseamnă, de i» tiuia, că adversarii acestora nu îşi mai îndeplinesc atribuţiile la fel i. laue ca până atunci şi, într-un fel, înregistrează eşecuri. Acest t... mi este valabil mai ales în privinţa acţiunilor deliberate care iiuplii a luarea prin surprindere, dar are o arie mai largă de cuci liniere73.

I neînd lucrurile la extrem, eşecurile din activitatea serviciilor I înhumaţii pot fi considerate similare celor din jocul de şah. i v mint, pentru perfecţionarea abilităţilor de şahist, este normal să i» analizate cât mai amănunţit stilurile de joc şi mutările individuale. În lui acesta, ar trebui să se amelioreze calitatea jocului individual în cazul în care cunoştinţele dobândite le sunt împărtăşite şi altora, ei vor juca, la rândul lor, mai bine. Per ansamblu, nu prittt* avea loc o creştere a numărului de jocuri de şah câştigate în raport t* numărul celor jucate. Desigur, în calitate de cetăţeni, nu ne inle resează o activitate de informaţii mai performantă în general, M încercăm să consolidăm capacitatea pe linie de informaţii a (ftrH noastre şi să o diminuăm pe cea a adversarilor.

*Soluţii instituţionale*. Printre soluţiile instituţionale avute ti vedere cel mai frecvent – soluţii care presupun restructurarea cadrului instituţional în care se desfăşoară activitatea serviciilor de informaţii se numără *analiza competitivă* şi crearea unui „avocat al diavolului”.

*Analiza competitivă* se referă la crearea unor centre analitic distincte în cadrul guvernului, fiecare dintre ele având dreptul de I formula şi a

transmite propriile evaluări informative. În principiu» fiecare centru ar urma să aibă drepturi egale şi generale de acces datele neprelucrate, indiferent de agenţia de informaţii care leobţinut. (în practică, dat fiind caracterul secret al anumitor tipuri d informaţii – de exemplu, informaţiile ce ar putea conduce la identl» ficarea unei surse umane –, acest lucru poate fi greu de realizat.)

De regulă, toate aceste centre, sau unele dintre ele, sunt părţi componente ale unor departamente şi agenţii guvernamentale importante sau ale unor servicii militare şi funcţionează, în primul rând, pentru a răspunde nevoilor speciale de informare ale organizaţiilor cărora le aparţin. De exemplu, în Statele Unite, Agenţia de Informa (l! a Apărării face parte din Departamentul Apărării şi este subordonat! atât şefilor Statului-Major Reunit, cât şi secretarului de stat al Apărării; fiecare serviciu militar are propriul comandament sau serviciu de informaţii; Departamentul de Stat are propriul Birou de Informaţii şi Cercetare. Într-o anumită măsură, competiţia dintre ele reflect! faptul că sunt subordonate unor departamente guvernamentale diferite, care uneori se află, la rândul lor, în competiţie.

Există, de asemenea, şi posibilitatea înfiinţării mai multor centre analitice *ad hoc* care să investigheze aceeaşi problemă. Două exemple de acest gen, care au fost date publicităţii, sunt cel al Echipelor A-B din 1975 – 1976 şi al Comisiei Rumsfeld din 1998. În primul caz, a fost creată o echipă de experţi (Echipa B) care să analizeze

ultimele evoluţii ale strategiei sovietice şi să confirme sau să infirme concluziile autorilor estimării naţionale de securitate din anul precedent (Echipa A) 74.

lit i el de-al doilea caz, o comisie condusă de Donald Rumsfeld a imlihil posibila ameninţare cu rachete balistice la adresa Statelor I unie venită din partea altor ţări decât Rusia şi China. Comisia a fost ttiftlii (îi (;1 în urma unei suspiciuni manifestate de membrii I inigfesul, i şi de alţi factori de decizie, potrivit căreia o estimare Niţlotmlil de securitate anterioară fusese prea optimistă75.

I lui lièrent dacă este efectuată în mod sistematic sau *ad hoc*, it. NMtJtjiil unei astfel de analize competitive constă, în primul rând, m (Mulbilitatea exprimării mai multor puncte de vedere la nivelulnte imilor de decizie, fapt ce conduce la o intensificare a dezbaterilor îi primite să se stabilească dacă informaţiile disponibile susţin fără un Invoc una dintre opinii. Astfel, analiza competitivă poate reprem mă o soluţie la problemele generate de acceptarea fără rezerve a. mm epţiilor convenţionale. În condiţiile existenţei unor centre analitice nu mente, creşte probabilitatea ca măcar unul dintre ele să maniile scepticism în privinţa opiniilor generalizate cu privire la o miumilă situaţie (deşi acest lucru nu este garantat), fiind, astfel, în măsură să determine celelalte agenţii să îşi justifice poziţia. Analiza

Miupeiitivă este o încercare de angajare – ţinând cont de cadrul 1 nu lat al reglementărilor

privind securitatea informaţiilor – într-un II Imul) de idei specific unei societăţi democratice care are ca rezultat promovarea cunoaşterii în general.

Astfel, riscul ca aceste centre să adopte puncte de vedere părtinitoare, sub influenţa orientării strategice a agenţiilor coordonatoare unu a restricţiilor bugetare, este relativ redus. Potrivit acestei argu-nientări, iniţierea unei dezbateri intense la nivelul diferitelor centre vu scoate în evidenţă netemeinicia punctelor de vedere care nu sunt instituite de dovezi, creând, în acelaşi timp, premisele necesare I nul ru ca o serie de idei noi, neconvenţionale să fie luate în considerare.

I) csigur, este posibil ca un anumit punct de vedere să fie adoptat iuţi o măsură relativ similară de diferitele structuri guvernamentale. Iuţi o astfel de situaţie, este puţin probabil ca simpla existenţă a unor centre analitice concurente să pună sub semnul întrebării ouccpţiile convenţionale, având în vedere că toate aceste centre ar fi dominate de acelaşi convenţionalism. Pornind de la această consideraţie, s-a propus crearea unui „avocat al diavolului” – altfel spus, i mici entităţi analitice având ca scop declarat contestarea punctelor de vedere general-acceptate.

Echipa B şi Comisia Rumsfeld reprezintă, totodată, exemple de „avocaţi ai diavolului” constituiţi *ad hoc* pentru a analiza o anumlift problemă, pornind de la premisa că o ipoteză anterioară legată de aceasta a fost eronată. Proiectul „avocatului diavolului” este o încercare

de instituţionalizare a acestei practici şi, implicit, de evitam a controverselor de natură politică de tipul celor ce au planat deasupra Echipei B, despre care unii critici au afirmat că ar fi exercitai o presiune externă nejustificată (altfel spus, politică) asupra procesului de analiză a informaţiilor76.

Deşi ambele instrumente instituţionale prezintă avantaje, niciunul dintre ele nu poate fi privit ca o soluţie universală sau, cel puţin, ca un pas în direcţia corectă. Într-un articol sugestiv intitulat „Why Intelligence Failures Are Inévitable”, Richard K. Betts arată că niciuna dintre soluţiile instituţionale sus-menţionate – şi nicio alin soluţie instituţională – nu poate preveni în totalitate eşecurile înregistrate în activitatea serviciilor de informaţii77.

Chiar dacă analiza competitivă poate da glas unor opinii diferite faţă de concepţiile convenţionale, opinii care, în caz contrar, nu ar putea fi exprimate, acest tip de analiză oferă factorilor de decizie o gamă largă de puncte de vedere, ceea ce îi poate pune în încurcătură sau îi poate determina să ignore toate informaţiile primite şi să se bazeze pe propriile opinii. De asemenea, este posibil ca obiecţiile prezentate de un astfel de „avocat al diavolului” instituţionalizat să îşi piardă capacitatea de a-i determina pe ceilalţi să îşi reconsidere poziţia tocmai pentru că exprimarea unui punct de vedere diferit intră în „atribuţiile sale”. Se poate ajunge, prin urmare, la un rezultat contrar celui urmărit, şi anume la situaţia în care anumite obiecţii justificate la

concepţiile tradiţionale sunt ignorate deoarece sunt considerate o atitudine normală şi previzibilă.

Aceasta nu înseamnă însă că măsurile instituţionale sunt lipsite de importanţă sau că modificarea lor nu poate fi benefică. Concluzia care se desprinde este că strategia optimă de organizare a serviciilor de informaţii nu poate fi stabilită fără a cunoaşte problemele sau deficienţele caracteristice aparatului de securitate naţională al unei ţări; stabilirea structurii organizatorice trebuie să ţină cont de modalităţile optime de contracarare a tendinţelor negative identificate. Aceeaşi soluţie – de exemplu, analiza competitivă – poate fi utilă sau nocivă, în funcţie de caracteristica generală a sistemului: la rt M icimil se caracterizează printr-un grad prea mare de conven-lei-ttiti Mii, analiza competitivă ar putea avea ca rezultat luarea în n»M) ilciare a unor puncte de vedere noi; în schimb, dacă există»Htllii (îi de a permite problemelor politice interne să domine strategia il* w ui iiaie naţională, poate fi necesară consolidarea unei structuri fi* în formalii unitare, care să aducă în prim-plan realităţile inter-iMi (loinile.

*Soluţii intelectuale*. Avantajul soluţiilor instituţionale este că pot M implementate pe cale ierarhică, prin directive şi decizii mana-g.» htir, totuşi, aceste soluţii nu atacă miezul problemei eşecului hi activitatea de informaţii, şi anume raţionamentul analistului. ÎmiMinAtăţirea raţionamentelor nu este un aspect care să poată fi miluiiouat prin măsuri administrative directe. Într-adevăr, dacă Îih în am să precizăm ce aspecte

trebuie urmărite, nu putem stabili

«imtudine nici măcar ce înseamnă „îmbunătăţirea raţionamen-miii”, în afara unui îndemn generic şi nu întotdeauna util de a fi uni inteligent”.

Deşi nu este posibilă stabilirea unor norme care să conducă ime uit abil la o analiză corectă a informaţiilor, ar putea fi util să îih neam identificarea deficienţelor sau erorilor intelectuale care pot 4 ferlii procesul analitic, fie în plan general, fie într-un anumit iiitiiicni şi loc. Astfel, putem să aflăm aceste tendinţe şi să încercăm, i în corectăm.

I»i între cauzele intelectuale ale eşecurilor înregistrate în activitatea i viciilor de informaţii, am văzut că o greşeală importantă care inamic evitată este tendinţa de a interpreta realitatea ca pe o reflexie.t jiu»priei imagini. Deşi toţi analiştii de informaţii pot comite această mare, ea reprezintă o problemă îndeosebi pentru comunitatea de minunaţii din Statele Unite. Americanii sunt înclinaţi să creadă că îmi oamenii au caracteristici similare, poate şi datorită experienţei ulcior Unite în asimilarea şi integrarea cu succes a imigranţilor cu înniialităţi şi credinţe religioase diferite. Astfel, analiştii serviciilor liinformaţii din SUA riscă mai mult decât colegii lor din alte ţări să v.ilueze şi să anticipeze acţiunile altora pornind de la ceea ce ar face i în circumstanţe similare.

Prin urmare, o măsură importantă de natură să remedieze această «i oure o constituie cunoaşterea aprofundată a altor societăţi şi

culturi.

Studiul limbii şi istoriei unei ţări, cunoaşterea tradiţiilor religioaso culturale ale acesteia pot contribui la creşterea semnificativă capacităţii de valorificare a informaţiilor. Trebuie întreprinse eforturi susţinute pentru a evalua situaţia internaţională nu numai din pe» spectivă proprie, ci şi din punctul de vedere al liderilor altor ţări.

Capitolul 4

În culise: operaţiunile secrete i «m punctul de vedere al opiniei publice, acţiunile secrete – în im t l-ai formele cele mai senzaţionale ale acestora, cum ar fi răsmimuea unui guvern sau asasinarea liderului acestuia – reprezintă imii ihn principalele forme de concretizare a activităţii serviciilor de minimalii; cu toate acestea, în viziunea specialiştilor şi cerce-Minţilor din domeniul informaţiilor, însăşi includerea acţiunilor mm iele în definiţia activităţii de informaţii este pusă sub semnul iniirbfirii. Această problemă este determinată de faptul că acţiunile mm ale presupun luarea unor măsuri de natură să afecteze politica în irmă a unei ţări, în timp ce activităţile de culegere şi analiză a idilelor se limitează la furnizarea informaţiilor care pot sta la baza I»În ic îi respective.

Ce sunt operaţiunile secrete?

În accepţia dată de comunitatea americană de informaţii, *acţiunile* în *me* reprezintă încercarea unui stat de a-şi îndeplini obiectivele de politică externă prin desfăşurarea unor activităţi secrete menite să inlliienţeze deciziile altui stat sau evenimentele şi circumstanţele de

iiuliii politic, militar ori social din altă ţară. După cum sugerează niiicuul, trăsătura definitorie a unei acţiuni secrete o reprezintă iiacterul său ascuns sau secret. Totuşi, definirea exactă a caracterului secret poate varia în funcţie de circumstanţe.

În unele cazuri, păstrarea secretului este, absolut necesară, iar guvernele se străduiesc să ia toate măsurile necesare astfel încât detaliile sau chiar şi simpla existenţă a activităţilor respective să în fie cunoscute decât de un cerc restrâns de persoane. Aceasta *H* întâmplă, de exemplu, în cazul în care o acţiune secretă vizerwÉ susţinerea unui grup de conspiratori ce urmăresc pregătirea mm lovituri de stat în altă ţară, prin introducerea ilegală a unor arme Im ţara respectivă. În alte cazuri, acţiunile în sine sunt cunoscute, dut guvernele implicate nu doresc să facă publică participarea lor I* acestea. Un exemplu de acest gen îl reprezintă finanţarea în secret, de către guvernul unei ţări, a unei publicaţii sau a unui post de radio care susţine politica sa ori manifestă o atitudine ostilă faţă de politic» adversarului său. În sfârşit, există şi situaţii în care o mare parte din informaţiile cu privire la operaţiuni sunt făcute publice, dar, din raţiuni diplomatice sau din alte motive, guvernele implicate evită n recunoască oficial participarea lor la evenimentele respective.

În Statele Unite, acţiunile secrete sunt definite în legislaţia actuali ca fiind „activitatea sau activităţile desfăşurate de Guvernul Statelof Unite în scopul de a influenţa situaţia politică, economică sau militari din alte ţări, rolul jucat de

[guvern] nefiind dezvăluit sau recunoscui public; astfel de activităţi nu includ... activitatea tradiţională de contrainformaţii... activităţile diplomatice... militare... [sau] ce ţin de domeniul aplicării legii" 1.

Conform acestei definiţii, se face distincţie între acţiunile secrete şi activitatea de culegere şi valorificare a datelor obţinute din surse secrete, cu alte cuvinte, de ceea ce, în Statele Unite, este considerată baza activităţii serviciilor de informaţii2. Diferenţa constă în faptul că obiectivul acţiunilor secrete nu este de a obţine informaţii, ci de a promova în mod nemijlocit obiectivele naţionale de politică externă. Din acest punct de vedere, se aseamănă într-o măsură mai mare cu alte instrumente de politică externă ale ţării, cum ar fi activităţile diplomatice sau operaţiunile militare, decât cu activitatea propriu-zisă a serviciilor de informaţii. În schimb, având în vedere că este vorba de o activitate desfăşurată în secret, care implică recurgerea la sprijinul unor aliaţi sau agenţi secreţi, se aseamănă mai mult cu activitatea de culegere a informaţiilor din surse umane decât cu alte strategii pe care le-ar putea pune în practică guvernul unei ţări.

Chiar dacă această definiţie este, în principiu, suficient de clară, nu e în totalitate exactă. De exemplu, deşi legea exclude în mod explicit activităţile „diplomatice", „militare", „de contrainformaţii".

t m' Îi. arc a legii" „tradiţionale" din definiţia acţiunilor secrete, nu fefliM ţic aceste activităţi şi nici nu stabileşte linia de demarcaţie mnim ric şi

acţiunile secrete. Şi acţiunile diplomatice, de pildă, au»4 km) influenţarea guvernelor şi oficialilor altor ţări şi sunt, de ai, oti, întreprinse în secret; de exemplu, adesea se impune ca»!». iwile dintre două ţări să fie desfăşurate în secret, fără ca alte pttt? i opinia publică să aibă acces la informaţii pe această temă. Este Umilul chiar ca subiectul anumitor discuţii purtate cu oficiali guver-MMintiali dintr-o ţară să nu fie adus la cunoştinţa altor membri ai lt-liila-i guvern.

hr asemenea, „activitatea de contrainformaţii" presupune *în* uiiicrea la serviciile unor agenţi dubli, după cum vom vedea în i – ...1111 următor. Aceşti agenţi urmăresc să obstrucţioneze eforturile

»! vii tarului de culegere a unor informaţii din surse umane, dar pot M iitih/nii şi pentru a-i transmite informaţii false, menite să îl inducă hi mare şi chiar să îl determine să îşi modifice planul de acţiune.

t»unul dublu trebuie să îşi înşele adversarul în privinţa activităţilor mii fapt ce influenţează, în mod inevitabil, activitatea de culegere îi indumaţiilor de către adversar.) Nu este clar în ce moment această tiviiaie „tradiţională" ar trebui să fie privită nu ca o activitate de i hiih, iiniormaţii, ci ca o acţiune secretă.

În plus, trebuie remarcat că sintagma *acţiune secretă* pare a fi o Invnilie americană, neexistând în vocabularul altor servicii de informihlii1 De exemplu, cel mai apropiat echivalent sovietic al acestei iliilu Kinc – *măsuri active* (*aktivnâie meropriiatiia*) – avea un sens mai inj» decât cel al

acţiunii secrete: se referea atât la „tehnicile des-Ii! m\ cât şi la cele secrete, aplicate în vederea influenţării eveni-m. ulcior, strategiilor şi acţiunilor altor ţări” 4. Conform acestei ili-lmiţii, măsurile active nu intrau în totalitate în sfera activităţii de mlitimaţii. În schimb, includeau alte activităţi de politică externă li lăturate atât de guvernul sovietic (de exemplu, activităţi di-pinmatice şi utilizarea unor mijloace de informare în masă oficiale, în îi ar fi Radio Moscova), cât şi de Partidul Comunist al Uniunii, va-lice (întreprinse, de exemplu, cu sprijinul partidelor comuniste, im alle ţări sau al unor grupări de faţadă precum Consiliul Mondial i I Vicii – World Peace Council). Sintagma punea un accent mai mare i «obiectivul urmărit – influenţarea situaţiei politice – decât pe «uacterul secret sau deschis al mijloacelor utilizatcă.

Indiferent de terminologia folosită, este important să reţinem 11 sensul dat de Statele Unite acţiunii secrete reprezintă doar una tllM numeroasele strategii de politică externă posibile. Datorită carm teristicilor sale unice, a suscitat de-a lungul timpului dezbateri aprinse, situându-se în prim-planul atenţiei tuturor; totodată, având în vedere caracterul său secret, ridică o serie de semne de întrebări în cazul unui guvern democratic. Se poate spune că alegerea termenului este oarecum nefericită, întrucât scoate în evidenţă o caracteristică I mijloacelor utilizate (caracterul lor secret), ignorând faptul că scopul urmărit e sau ar trebui să fie cel de îndeplinire a obiectivelor dl politică externă. Din

cauza accentului pus pe formă, în detrimentul obiectivului urmărit, dezbaterile desfăşurate în Statele Unite pl, marginea acţiunilor secrete s-au concentrat, în principal, asupra legalităţii şi asumării răspunderii, fiind trecute sub tăcere alte aspecti fundamentale, referitoare la obiectivele şi strategia de politică externă, în acest capitol, acţiunile secrete vor fi tratate atât ca o componentă a activităţii serviciilor de informaţii, cât şi ca un instrument dl politică externă; în capitolul 6, vor fi abordate aspectele specifici referitoare la desfăşurarea unor acţiuni secrete de către un guvern democratic. Ţinând cont de ambiguitatea definiţiilor mai vechi, şi mai noi ale acţiunilor secrete, în continuarea prezentului capitol vor fi analizate activităţile cu o aplicabilitate mai largă decât acţiunile secrete, pentru a clarifica limitele acestora din urmă. O definiţie mal satisfăcătoare a acţiunilor secrete ar trebui să se detaşeze într-o mai mare măsură de inconsecvenţele legislative şi procedurale din Statele Unite; o astfel de definiţie nu a fost însă identificată până în prezent.

Tipuri şi exemple de acţiuni secrete în sensul său cel mai larg, de influenţare prin mijloace secrete a evenimentelor sau circumstanţelor din altă ţară, sintagma *acţiune secretă* include o gamă largă de activităţi, de la cele prozaice, de genul acordării de asistenţă tehnică secretă (ca, de exemplu, cursuri de perfecţionare sau furnizarea unor echipamente de comunicaţii ori asigurarea securităţii) unui guvern străin prieten, până la cele mai spectaculoase, cum ar fi asasinarea unui

lider sau instigarea ori iptllnitni unei lovituri de stat. Este aşadar dificil de redactat o listă fettttnă a tipurilor de acţiuni secrete desfăşurate de agenţiile de trilionul) i în plus, agenţiile de informaţii din Statele Unite nu au (femhin o tipologie-standard a acţiunilor secrete şi nu dispun de şi Hihil specializat care să analizeze această chestiune. În continuare Mii tiu crea să elaborăm o astfel de clasificare.

opul acţiunilor secrete este de a influenţa acţiunile unor guverne sau evenimentele ori circumstanţele din altă ţară. Aceste unt pot viza guvernul ţării respective, populaţia în general sau un iMMinii segment al ei. În ţările democratice, efectele acţiunilor de Influenţare a populaţiei sunt, de cele mai multe ori, resimţite şi de luve» nul ţării respective; pe de altă parte, astfel de acţiuni pot avea tiMpoiiante consecinţe pe termen lung în ţările nedemocratice sau cu linme totalitare.

lulluenţarea strategiilor, evemmentelor sau circumstanţelor din «li. (Ali constituie însăşi esenţa politicii externe; acţiunile diplo-hi. Îi îi r urmăresc, în aceeaşi măsură ca acţiunile secrete, îndeplinirea în i Hiui obiectiv. Este, de asemenea, posibilă trimiterea sau staţionarea în uni trupe militare pe teritoriul altui stat în scopul influenţării iiMlegici sale; aceasta este o măsură obişnuită pe timp de pace, dar [Hiute li aplicată şi pe timp de război. Prin urmare, nu este surprin-rtioi faptul că multe dintre tehnicile de acţiune secretă analizate mai on pol li puse în practică şi prin mijloace nesecrete. Din punctul de o ilnc al Guvernului american, includerea unei acţiuni în

categoria di „secretă” depinde adesea nu atât de natura cazului, cât de parii»ularităţile definiţiilor juridice şi administrative ale acţiunii mi icte.

Sprijinul secret acordat guvernului unui stat prieten

În multe cazuri, acţiunile secrete sunt întreprinse pe baza unei alianţe l-ai ne cu persoane sau grupări care urmăresc aceleaşi obiective, viisi lucru este mai uşor de pus în practică atunci când aliatul în auzii este guvernul unui stat prieten. În acest caz, acţiunile secrete pol li limitate la activităţi lipsite de senzaţional, cum ar fi acordarea în asistenţă în secret statului aliat sub forma garantării siguranţei pn sonate a liderului său sau a furnizării unor echipamente de miiunicaţii securizate (criptate).

*Asistenţa care nu implică activităţi de informaţii*. Există \m motiv pentru care astfel de activităţi sunt incluse în categoria acţiunii»* secrete. Sprijinul acordat guvernului unui stat prieten îl ajută acesta să se menţină la putere şi, prin urmare, influenţează cui Mii evenimentelor din ţara respectivă. În plus, acţiunile se desfăşoară!* secret – cu alte cuvinte, datele, informaţiile cu privire la sprijinul acordat nu sunt făcute publice, iar în cazul în care se produci ti scurgere de informaţii, guvernul nu îşi va asuma public respoft stabilitatea. Dar astfel de acţiuni pot fi incluse la fel de bine şi în categoria acţiunilor diplomatice secrete. De fapt, sintagma *acţiuni secretă* se aplică, probabil, acestui gen de activitate doar dae a operaţiunea a fost întreprinsă de o agenţie de informaţii; furnizanHI

de asistenţă în secret prin intermediul personalului diplomatic suini în tar nu va fi, probabil, inclusă în această categorie.

Astfel de activităţi sunt, de obicei, realizate la scară redusă l relativ necontroversate, motiv pentru care publicarea în presa seri»! a unor informaţii pe această temă este puţin probabilă. Totuşi, cil pot prezenta importanţă atât din punct de vedere tehnic (prin furnizarea capacităţilor necesare guvernului statului prieten, pe care aceşti nu le-ar fi putut obţine prin forţe proprii), cât şi psihologic (ca o dovadă a credibilităţii şi eficienţei sprijinului acordat guvernului respectiv). Dar această lipsă a vizibilităţii şi a controverselor nu se manifestă întotdeauna.

În primul rând, este posibil să apară divergenţe cu privire în statele ce trebuie considerate prietene şi eligibile pentru acordare» de asistenţă, la fel ca în cazul asistenţei deschise. Caracterul secret nu modifică natura acestor divergenţe, dar poate crea suspiciuni în rândul oponenţilor unui program, ce pot bănui că principalul motiv pentru care programul a fost ţinut secret a fost de a evita formularea unor obiecţii la adresa lui.

În al doilea rând, pot apărea discuţii cu privire la tipul de asistenţă acordată, în special dacă statul beneficiar are o reputaţie îndoielnică 1. De exemplu, în 1974, Congresul Statelor Unite a interzis acordarea unor fonduri altor state pentru instruirea forţelor de poliţie; această decizie a fost adoptată pe fondul unor controverse cu privire la încălcarea drepturilor omului de

către regimurile din America Latină care beneficiaseră de astfel de fonduri7.

*hhn eu pe linie de informaţii*. Un alt tip de asistenţă acordată

Cnunului unui stat prieten îl reprezintă furnizarea sau schimbul de tumulii provenite din surse secrete. Având în vedere că aceasta te fi activitate de rutină, nu ar trebui să fie inclusă în categoria ¥ lmil h h secrete. În situaţiile care presupun un schimb de informaţii 01 în valoare aproximativ egală, scopul furnizării unor date altui stat ni»! în tla de a primi în schimb alte informaţii relevante, această hoiţiuiie ar trebui să fie inclusă, mai degrabă, în categoria acti-l iuţilor de culegere a informaţiilor decât în cea a acţiunilor secrete. Ihiusa, în situaţiile în care furnizarea informaţiilor are loc într-o mimiia direcţie, principala motivaţie a statului care le transmite fu”!? li intenţia de a ajuta celălalt stat. În acest caz, activitatea imhh 11 vă poate fi considerată sprijin secret acordat unui stat prieten, vătul în vedere că permite altui stat să îşi îndeplinească anumite MIIIM iive pe care nu le-ar fi putut atinge prin mijloace proprii şi se iMiny»ară în secret8.

I»rei, în general, schimbul de informaţii are loc doar între state» miMilerate prietene (statul care furnizează informaţiile consideră că ttMitlhtarea statului beneficiar este şi în interesul său), există nume-exemple de situaţii în care un stat i-a transmis informaţii altuia h» nu este considerat prieten pentru a-l determina sau a-l provoca să miopie o anumită decizie, care să fie în interesul ambelor părţi. Ai Rusia situaţie, care

presupune nu atât acordarea de asistenţă altui h.îi, rât determinarea adoptării de către acesta a unei anumite măsuri, mir prezentată mai jos ca fiind o metodă de influenţare a percepţiei mihi stat cu privire la poziţia sa pe plan mondial.

Influenţarea opiniilor altui stat pic deosebire de situaţiile prezentate mai sus, în care sprijinul în dat guvernului altui stat porneşte de la premisa că acesta poate mi ibui la promovarea propriilor interese, cel mai frecvent şi mai

«îi, icteristic tip de acţiune secretă vizează influenţarea opiniilor altui lat, în scopul modificării strategiei, evenimentelor sau circum-iantelor din ţara respectivă în folosul propriilor interese. Acest ihiectiv se realizează fie prin influenţarea acţiunilor guvernului h.pectiv, fie a opiniei publice din ţara respectivă sau a unor grupuri i sectoare ale sale, independent de acţiunile guvernului respectiv şi, adesea, împotriva intenţiilor acestuia. Scopul final îl constitui» influenţarea politicii guvernului respectiv sau crearea condiţill»* necesare pentru schimbarea acestuia. În această secţiune şi în secţiunoi următoare este prezentat modul în care acţiunile, evenimentele ftiti circumstanţele pot fi afectate prin influenţarea (1) opiniilor guvernului altui stat sau (2) opiniilor anumitor segmente ale populaţiei din stalul respectiv, cu privire la aspecte de ordin politic, militar sau economi

*Agenţii de influenţă*. Metoda cea mai simplă şi mai directă de influenţa acţiunile unui guvern străin este de a recurge la *agenţi* (*h influenţă* – agenţi a căror principală misiune constă nu în

culegeroi informaţiilor, ci în influenţarea directă a politicii altui stat. Având în vedere că un agent care deţine o funcţie importantă în guvernul altul stat ar putea îndeplini ambele obiective, această distincţie este mul mult de natură teoretică decât practică. În astfel de cazuri, cil» posibil ca utilizarea unui agent cu atribuţii pe linie de culegere dl informaţii în scopul influenţării politicii guvernului ţării sale să nu fie considerată acţiune secretă. Totuşi, un serviciu de informaţii ar putea să nu se arate dispus să pună în pericol o sursă de informalll utilă trasându-i sarcina de a încerca să influenţeze politica guvernului său dacă, prin acţiunile lui, agentul respectiv ar putea atrage atenlla asupra sa.

Agentul de influenţă poate fi un oficial guvernamental sau un membru marcant al clasei politice din ţara-ţintă (altfel spus, o persoană din interior), ce are acces la alţi oficiali guvernamentali, la liderii de opinie şi la mass-media. Dacă agentul de influenţă este un înalt oficial din cadrul guvernului-ţintă, ar putea fi în măsură să întreprindă, pe cont propriu, acţiuni în beneficiul altui stat. Totuşi, situaţia cea mai frecventă în cazul unui guvern birocratic este ca agentul să îşi determine colegii să adopte anumite politici care să susţină interesele altui stat. Evident, el nu poate promova în mod deschis politicile respective admiţând că ele sunt în beneficiul unei puteri străine, potenţial ostilă, ci trebuie să încerce să influenţeze opiniile colegilor să-i cu privire la situaţia politică în aşa fel încă! aceştia să considere necesară susţinerea

strategiilor ce avantajează statul al cărui agent este.

De exemplu, în anii ’30—40, serviciile de informaţii sovietice aveau câţiva agenţi care lucrau în cadrul Guvernului Statelor Unite?

ttititM» t ci mai importanţi se numără Harry Dexter White, angajat al tfeţ MIMmentului Trezoreriei. Cu timpul, White a fost promovat în HM» pu ilr secretar-adjunct al Trezoreriei, cea de-a doua funcţie ca «qHHiitnia din cadrul Departamentului. Pe lângă furnizarea unor EIN» l Mvrele serviciului de informaţii sovietic, White acţiona şi ca iştii ilr miluenţă. Astfel, în pregătirea conferinţei de la Ialta din Mn. Miir 1945, unde s-au întâlnit Stalin, Roosevelt şi Churchill, M! r fi avut iniţiativa redactării unei propuneri a Departamentului liMHIPI ici privind acordarea unui important împrumut pe termen de M am, cu dobândă redusă, Guvernului de la Moscova şi alocarea «imn Malc din suma propusă de douăzeci de miliarde de dolari, pe t Ici mania ar fi urmat să o plătească drept despăgubiri de război, li. (iltin, White a făcut un apel (pe aceeaşi linie cu poziţia Uniunii… viiie) la distrugerea totală a capacităţilor industriale chimice, ilfiiilic şi metalurgice ale Germaniei: „În opinia mea, cea mai în Mrt mi xlalitate de a consolida încrederea sau neîncrederea în relaţiile Hulit Statele Unite şi Rusia o reprezintă poziţia pe care acest guvern îi va adopta în privinţa Germaniei”. Totuşi, în acest caz, eforturile liaomiinse de White în interesul Uniunii Sovietice au fost parţial.» în ale de opoziţia manifestată de Departamentul de Stat. În

cele Un în mă, nu s-a acordat niciun împrumut masiv, iar Germania nu *4* hm dezindu-strializată. Cu toate acestea, Roosevelt a aprobat... lor în propunerilor înaintate de White şi împotriva voinţei lui hun liill, valoarea despăgubirilor de război care fusese stabilită de Huhia, precum şi partea ce urma să-i revină acesteia10.

H n agent de influenţă din timpul Războiului Rece a fost nor

— Planul Arne Treholt, funcţionar în cadrul Ministerului de Externe dui (ara sa şi, timp de peste un deceniu, agent sovietic. Profitând de un iulie deţinute în minister şi la Naţiunile Unite, Treholt a încercat.

— Mile câte ori i s-a ivit ocazia, să modereze sau să modifice politicile iun sale în beneficiul Uniunii Sovietice. De exemplu, la începutul h nici sale, Treholt a fost numit într-o funcţie relativ importantă în uliul conferinţelor de drept maritim şi a făcut parte din delegaţia» «»i veiană care a purtat negocieri cu Moscova pe tema apelor i i iioriale şi a drepturilor de pescuit în Marea Barents. Potrivit unei» luni, „Treholt nu numai că a informat permanent KGB cu privire i «poziţia Norvegiei în cadrul negocierilor, ci a acţionat şi ca agent Imiluenţă în echipa norvegiană de negociatori”, contribuind la elaborarea unui tratat „care a fost aspru criticat în Norvegia pe ihm». că favoriza interesele Uniunii Sovietice”. În general, Treholt a hvtn uz de diferitele funcţii deţinute în cadrul ministerului pentru promova o serie de politici – cum ar fi cea a unei Zone Nortll* Libere de Arme Nucleare – care susţineau eforturile

Uniunii Sov în vizând îndepărtarea Norvegiei de Alianţa Nord-Atlantică (NAlt l Treholt a jucat un rol deosebit de important în relaţia cu prM norvegiană, utilizându-şi numeroasele contacte din mass-media pe în «a promova o atitudine antiamericană şi anti-NATO. Când a arestat, în 1984, Treholt era şeful Biroului de presă şi comunicau din cadrul Ministerului de Externe”.

Un alt agent de influenţă din timpul Războiului Rece, recrutat afara aparatului guvernamental, a fost Pierre-Charles Pathé, cetă (ea a francez cu relaţii importante în cercurile politice, care, în 1979, fost găsit vinovat de spionaj în favoarea Uniunii Sovietice condamnat la cinci ani închisoare. Fiind un apropiat al cercurika politice, deţinea multe informaţii despre politica de la nivel înalt, precum şi despre viaţa personală a multor oameni politici, chlai dacă nu avea acces la informaţii secrete. Totuşi, se pare că adevărata sa infracţiune nu a constituit-o spionajul, ci acţiunile întreprinse la calitate de agent de influenţă.

În 1976, beneficiind şi de o finanţare primită de la KGB, a lansat un buletin informativ politic ce purta numele *Synthèse*. Pe parcursul următorilor trei ani, această gazetă, ce era citită de o mare parte din elita politică a Franţei (la un moment dat, 70% din membrii Cameral Deputaţilor erau abonaţi ai gazetei), a denigrat şi a atacat intereseli şi politica occidentale, diferenţele foarte mari dintre interesele l politica Franţei, pe de o parte şi cele ale celorlalte state membre ale Alianţei Nord-Atlantice (în special, ale Germaniei Federale şi

Statelor Unite), pe de altă parte, şi a susţinut poziţia Uniunii Sovietice şi a aliaţilor să-i pathé a fost arestat după ce a fost surprins în momentul în care primea bani de la un ofiţer KGB cu ocazia unei întâlniri clandestine ce a avut loc într-o suburbie a Parisului12.

Natura relaţiei dintre un serviciu de informaţii şi un agent de influenţă variază în funcţie de circumstanţe. În cazul unei persoane ca Pathé, jurnalist prestigios şi apropiat al cercurilor politice, a cărui simpatie pentru Uniunea Sovietică data de dinaintea oricărei relaţii clandestine cu KGB (probabil că el a fost remarcat de KGB după* publicarea, în 1959, a unui articol în favoarea Uniunii Sovietice).

«mm la probabil, flexibilă, bazată pe interese comune, nu rigidă, yul pe iiansmiterea unor instrucţii detaliate.

h«iuimi tic la categoriile identificate de serviciile secrete ale I Inimii Sovietice, putem distinge mai multe tipuri de agenţi de «fiu Miin, în funcţie de gradul şi tipul de control exercitat asupra Minţii tic serviciul de informaţii. Din prima categorie fac parte jaloanele de încredere” – cu alte cuvinte, persoanele care sunt! în m r să colaboreze cu un guvern străin pentru a promova anumite gttH-tiive pe care le împărtăşesc, dar care nu sunt receptive la MIM iiicii unor instrucţii detaliate şi, în general, nu sunt remu – hii e alia categorie este cea a agenţilor „controlaţi”, care primesc îi h ulii ordine precise şi cărora, de obicei, li se acordă o recompensă Miniuh litră pentru serviciile lor. La polul opus se află persoanele care

unii manipulate (de pildă, prin intermediul unor consilieri sau al mm prisoane din anturaj) să întreprindă anumite acţiuni în interesul iJuil Mul, dar care nu sunt conştiente de acest lucru13.

*Informarea şi dezinformarea*. O altă metodă de influenţare a

* (lunilor unui stat constă în furnizarea anumitor informaţii (adevărate mo lui se) menite să îl determine să întreprindă un anumit gen de acţiuni. I'm t' Hemplu datează din 1983, când Statele Unite i-au transmis feftiolahului Khomeinr informaţii cu privire la „prezenţa unor agenţi îi, iil, iboratori sovietici în Iran". Această informaţie a provocat două nu, de execuţii şi „desfiinţarea partidului comunist Tudeh", fapt ce

* dal i» lovitură majoră operaţiunilor KGB şi influenţei sovietice" în Iran. Maihr l Iniţe obţinuseră, se pare, această informaţie de la un „diplomat" *uns* irile din Teheran, Vladimir A. Kuzichkin, care a imigrat în Marea Hi iiame în 1982; Kuzichkin era, de fapt, „un ofiţer superior KGB...

m avusese misiunea de a ţine legătura cu partidul Tudeh" 14.

I»ieşi, în acest caz, CIA a fost, se pare, implicată, nu este obligau me recurgerea la serviciile secrete pentru a transmite astfel de lui» hmaţii. În lipsa implicării serviciilor de informaţii, o astfel de in nviiate nu ar fi, probabil, considerată acţiune secretă, deşi natura i-a i amâne, în principiu, aceeaşi. Un exemplu de asemenea activitate, h. nu poate fi inclusă în categoria acţiunilor secrete, l-a reprezentat

Ayatolahul Khomeini (1902 – 1989), lider religios iranian şi liderul politic. Îl revoluţiei iraniene din 1979 care a dus la răsturnarea şahului Iranului, Mohammad Reza Pahlavi (n.r.).

Încercarea prim-ministrului britanic, Winston Churchill, în aprilie I M4 de a avertiza Uniunea Sovietică cu privire la iminenţa atacului Genne»W

În contextul istoric respectiv, este uşor de înţeles de ce Stulln pus sub semnul întrebării motivele lui Churchill. Stalin, care avaa probabil, o părere preconceptă cu privire la duplicitatea engic/lk* a tras concluzia că era în interesul Marii Britanii ca relaţiile du tu Uniunea Sovietică şi Germania să se înrăutăţească. Churchill ape în probabil, că măsurile defensive luate de Uniunea Sovietică pe hm acestei informaţii ar putea fi interpretate drept o ameninţare É Germania, care s-ar fi simţit obligată să îşi întărească dispozitiv»I» militare la graniţa sovietică. În consecinţă, Stalin a considera!» i acest avertisment este o diversiune şi l-a ignorat15.

Dacă aceste două exemple menţionate mai sus presupun transmiterii unor informaţii reale, dezinformarea poate da rezultate la fel de bune, atât timp cât informaţiile transmise sunt plauzibile. De exera piu, în timpul Războiului din Vietnam, Statele Unite au încercat l creeze impresia că o mişcare de gherilă anticomunistă acţiona la Nordul Vietnamului. Scopul acestei dezinformări era de a determina Vietnamul de Nord să pună la îndoială eficacitatea aparatului, său intern de securitate. De fapt, aşa-numita „Sfântă Sabie a Ligii Patrioţilor” (Mat Tran Guom

Thieng Ai Quoc în vietnameză, Sacrul Sword of the Patriots League în engleză – SSPL) era formată dilt ţărani care fuseseră răpiţi din Vietnamul de Nord, duşi într-un sat aparent „eliberat” (de fapt, aflat sub controlul Vietnamului de Sud), îndoctrinaţi cu principiile SSPL, instruiţi şi apoi infiltraţi în Vietnamul de Nord pentru a „răspândi vestea” despre ligă. Timp de patru ani, în anii ’60, peste o mie de persoane din Vietnamul de Nord au foit capturate şi apoi trimise înapoi având asupra lor materiale, documente şi informaţii cu privire la SSPL, menite să susţină stratagema”.

O altă tehnică de dezinformare este aşa-numita „dezinformare tacită prin documente falsificate”, care presupune transmiterea pe căi neoficiale a unui document falsificat către un guvern străin, fără a face public documentul respectiv. În cel mai bun caz, guvernul-ţintfl (a cărui influenţare se urmăreşte) acceptă documentul falsificat ca fiind autentic şi nu întreprinde alte investigaţii. Guvernul care se presupune că ar fi emis documentul în cauză nu ştie nimic despre acesta şi, prin urmare, nu poate să-i nege autenticitatea.

O încercare de acest gen, care a eşuat pentru că guvernul-ţintă a făcut investigaţii, este descrisă de Ladislav Bittman, fost agent ceh

* înhumain. Potrivit relatării sale, în 1977 sovieticii au redactat un fotwtiaiulum contrafăcut, care ar fi fost, aparent, emis de Ambasada iumlmi Unite la Teheran şi au făcut în aşa fel încât să fie trimis Himtim la Ambasada Egiptului din Belgrad.

Memorandumul, care Alf M inenliunea „Strict Secret”, prezenta un presupus complot pus în mlr de Statele Unite, Iran şi Arabia Saudită pentru a-l răsturna pe MIM llutcle egiptean Anwar Sadat. Acţiunea secretă a eşuat deoarece Îimv, mul egiptean a solicitat oficial lămuriri de la Washington şi a ptmii un răspuns care l-a convins că memorandumul era contrafăcut17.

Vrastă formă de dezinformare poate viza direct serviciul de Nilhimain din ţara-ţintă. În acest caz, informaţia falsă nu este transmua yaivernului-ţintă, ci e lăsată, cum s-ar spune, la îndemână, ritt în a li descoperită de serviciile de informaţii; de exemplu, pot pullule convorbiri de natură să creeze o impresie greşită, de la Utumite posturi telefonice despre care se ştie că sunt interceptate de invit ml de informaţii din ţara-ţintă. O asemenea campanie de iMnlormare este cunoscută sub numele „diversiune” şi inclusă în rtflegorin activităţilor de contxainformaţii, nu a acţiunilor secrete.»V paulă distincţie este însă oarecum arbitrară, în condiţiile în care K opul şi metoda de lucru sunt, în linii mari, aceleaşi. În schimb, o am hl de operaţiune reprezintă o modalitate de obstrucţionare a nilvliăţilor de culegere şi analiză a informaţiilor desfăşurate de»n vu lui de informaţii din ţara-ţintă; ea se bazează pe o cunoaştere»Îi inhala a surselor şi metodelor de acţiune ale serviciului de informaţii vizat. Din acest punct de vedere, este firească includerea sa în ttu»oria activităţilor de contrainformaţii.

Influenţarea opiniilor populaţiei din alt stat

pir deosebire de tehnicile prezentate până acum, cele descrise în i niitinuare vizează în principal influenţarea opiniei publice din altă (.111 Având în vedere caracterul relativ vag al acestei sarcini, rezultatele

«h ic re te obţinute în urma aplicării acestor tehnici sunt mai dificil de «valuat. Deşi multe dintre exemple pot părea nesemnificative luate parat, efectul general pe termen lung asupra opiniei publice este înnificativ. Prin urmare, aceste tehnici sunt utile în cazul în care imvernul care le aplică este conştient de faptul că se angajează nu un proces de durată şi sunt mai puţin indicate în cazul unui guvern ce abordează fiecare problemă sau situaţie de criză ca pe im eveniment de sine stătător.

*Agenţii de influenţă*. Deşi această tehnică presupune, în uimi normal, utilizarea unor agenţi care să poată influenţa, mai mult sau mai puţin direct, opiniile şi strategiile guvernului, există şi agenţi I căror principală misiune constă în influenţarea opiniei publice din altă ţară. Potrivit unui fost ofiţer KGB, Franţa a reprezentat un tenw propice pentru acest gen de activităţi: „Majoritatea agenţilor francoil cel mai bine cotaţi de la jumătatea anilor ’70... erau jurnalişti sau aveau relaţii strânse cu presa”. Recurgând la agenţi şi colaboratori din rândul presei franceze, serviciile de informaţii sovietice au exploatat cu succes tendinţele comuniste şi gaulliste manifestate dl o parte a opiniei publice din Franţa, pentru a submina relaţiile dinţii această ţară şi celelalte state membre NATO şi pentru a consolida

sprijinul populaţiei în favoarea intensificării relaţiilor de prietenie cu Uniunea Sovietică18.

Stanislav Levchenko, maior KGB care a imigrat în Statele Unita în 1979, a relatat câteva exemple de situaţii în care Uniunea Sovietici a utilizat agenţi de influenţă pentru a influenţa presa şi strategia politică din Japonia 19. Printre acestea se numără: utilizarea unul membru marcant al Partidului Socialist Japonez pentru a împiedica alt membru al aceluiaşi partid, pe care KGB îl credea agent chinez, să obţină o funcţie de conducere; utilizarea unui corespondent al ziarului *Yomiuri* din Tokio pentru a promova publicarea unui articol având ca scop eliberarea unui agent sovietic al Serviciului de Informaţii Militare (GRU) care fusese arestat în urma unei operaţiuni întreprinse de un agent dublu; utilizarea unui tânăr corespondent american al agenţiei Associated Press pentru a publica o aşa-zisă scrisoare trimisă de soţia unui pilot al forţelor aeriene sovietice care fugise din Siberia în Japonia la bordul avionului său, MIG-25, în care aceasta îl implora să se întoarcă în Uniunea Sovietică20.

*Propaganda anonimă*. Una dintre cele mai directe metode de influenţare a opiniei publice o reprezintă popularizarea unor puncte de vedere, date adevărate sau false prin intermediul mijloacelor de informare în masă – cu alte cuvinte, prin propagandă (aşa cum este denumită peiorativ). De exemplu, ţările cu o politică externă activă tilt» olmci, propriile posturi de radio (cum ar fi *Vocea Americii*, fu *Moscova* şi altele) care exprimă făţiş opiniile acestora pe HHiikm unor

probleme internaţionale, la fel cum editorialele exprimă pu» li în de vedere ale redactorului sau editorului publicaţiei respective.

Ililuţfi, pot exista situaţii în care un guvern nu doreşte să fie îmi im direct cu materialul inclus în propagandă. În astfel de cazuri, phiii pune în circulaţie anumite opinii sau relatări într-o manieră… disimuleze originea lor. Acest lucru este posibil fie prin *m*¥\ui ca lor în publicaţii pe care nu le deţine sau nu le controlează, fi {Hin includerea în publicaţii considerate de opinia publică înde – (»mimle, dar care sunt, de fapt, controlate de guvern21.

Itxlstă două motive majore pentru care un guvern poate recurge I* piopaganda anonimă. În primul rând, este posibil ca publicul-ţintă» «t hr mai dispus să accepte propaganda dacă originea acesteia e ilhuuulaia, iar substratul nu este evident. De exemplu, propaganda, li»lfl»urată de Marea Britanie în Statele Unite înainte de intrarea Anin ic îi în Primul şi în cel de-al Doilea Război Mondial s-a bazat mii nea pe mecanisme secrete pentru a da impresia unei relatări luniive şi independente a unei ştiri. De exemplu, recurgând la Miiigiuiiţi din Europa Centrală, serviciile de informaţii britanice au m-ii) H să se infiltreze în mai multe operaţiuni clandestine desfăşurate iii (Germania în Statele Unite. Pentru a diminua tendinţele izolaţii misie şi a provoca antipatia opiniei publice americane faţă de i în i mania, informaţiile referitoare la aceste operaţiuni au fost transmue de britanici redactorului-şef al publicaţiei *Providence* (*R.I.*) *tocmai*. Pe baza

acestor informaţii, ziarul a publicat ulterior o serie în articole care au fost preluate şi de alte periodice din Statele i linte; se pare că redactorii publicaţiilor respective au crezut că o laurile erau bazate pe investigaţii prealabile întreprinse de jur-u.iliştii în cauză22.

l în al doilea motiv pentru utilizarea mecanismelor de propagandă neagră" este că, din considerente diplomatice, un guvern poate iloii să nu fie asociat cu anumite opinii pe care totuşi intenţionează a le transmită unui anumit public. De exemplu, în timpul crizei u.iniene a ostaticilor din perioada 1979 – 1981, guvernul sovietic a uloptat o poziţie corectă din punct de vedere diplomatic, condam-uand luarea de ostatici la ONU, în vreme ce postul său de radio secret, *Vocea Naţională a Iranului*, a aprobat-o pe deplin, încerc Aml să stârnească sentimente antiamericane în Iran23.

În afara presei pentru propaganda „neagră", ale cărei origliit trebuie să fie ascunse, se poate vorbi şi despre o propagandă „gri", ale cărei origini nu sunt recunoscute public, deşi nu sunt tăinuite tf deplin sau eficient. Spre exemplu, Guvernul Statelor Unite a în Tiin (în *Radio Europa Liberă* şi *Radio Libertatea* în 1949, respectiv în 1931, pentru a emite în Europa de Est şi Uniunea Sovietică. Spre deosebiri de *Vocea Americii*, aceste posturi de radio nu aveau ca scop transmiterii poziţiei oficiale a Statelor Unite, ci urmau să ofere populaţiilor vizate atât informaţii despre propriile ţări, care nu erau disponibili în presa locală, controlată de guverne, cât şi

informaţii despre Occident. Ele erau înfiinţate ca organizaţii americane private; ti) sprijinul acestei acoperiri, făceau chiar apeluri publice, solicitând fonduri. De fapt, aceste posturi erau conduse de către CIA. Potrivii lui Ray Cline, „CIA a organizat acest demers... considerând el posturile de radio ar fi mai eficiente dacă legătura lor cu Guvernul Statelor Unite ar fi ascunsă" 24. Dar, deşi legăturile cu Guvernul american nu erau recunoscute, era evident că posturile de radio făceau parte dintr-o operaţiune americană25.

O altă metodă de a face propagandă fără ca ea să fie asociat! entităţii care o generează implică transmiterea unor ştiri în medii independente sau scrierea şi publicarea unor cărţi de către autori şi edituri ce nu au legături evidente cu guvernul ori cu agenţiile sale de informaţii. De exemplu, într-o campanie bazată pe acţiuni secrete împotriva influenţelor comuniste în Europa Occidentală derulată în timpul Războiului Rece, CIA s-a folosit de o propagandă care nu putea fi atribuită unei anumite entităţi, inclusiv subvenţionând în secret publicarea unor cărţi şi articole transmise prin intermediul agenţilor de influenţă ce lucrau pentru agenţiile de ştiri sau pentru ziare.

Una dintre cele mai cunoscute activităţi de acest gen ale CIA a fost publicarea, în diverse ziare din afara Statelor Unite, a unei copii furnizate de Agenţie a „discursului secret" din 1956, prin care Hruşciov condamna „cultul personalităţii" al lui Stalin26. Un alt exemplu este sprijinul acordat de CIA pentru redactarea şi publicarea lucrării *The Penkovsky Papers*,

constând într-o relatare, bazată pe materiale, a cazului real al prunului spion CIA în Uniunea Sovietică, de la finele anilor ’50 şi începutul anilor ’6027.

I» irimică asemănătoare constă în utilizarea unei grupări-paravan II Minim de propagandă. Acest tip de grupări, deşi aparent au o *urea* i/ispândire, sunt, de fapt, sub controlul unui guvern şi se poate t + uiia pe ele că vor adopta poziţii corespunzătoare obiectivelor «o mi Im. Aşadar, ele îndeplinesc aceeaşi funcţie ca propaganda nu poate fi atribuită unei anumite entităţi – exprimă opinii care Hi»vrii interesele unui guvern, dar într-o formă ce le poate face trupiabile pentru un anumit public. Spre exemplu, înaintea celui *fh* il 1»oilea Război Mondial, britanicii au înfiinţat mai multe grupări-ţiehiv, în al căror obiectiv era să combată şi să hărţuiască America I a-i, teamai mare şi mai importantă organizaţie izolaţionistă din tMU le Unite28.

*falsurile*. O altă tehnică de a pune în circulaţie materiale fără, mimarea răspunderii pentru ele constă în crearea şi transmiterea am h documente falsificate29. Ca şi în cazurile discutate anterior... asta tehnică serveşte acelaşi obiectiv general: de a influenţa în o rpţiile unui public-ţintă, astfel încât acesta să ia măsurile dorite. Manualele utilizate în acest sens – ce pot consta în argumentele pu /cutate de către un agent de influenţă, conţinutul propagandei i.m* poate fi atribuită sau nu unei entităţi ori textul falsului – trebuie tfllie plauzibile pentru cei care se încearcă a fi influenţaţi. Prin urmare, în general

ne aşteptăm ca în materialul falsificat să fie în m «aţe elemente de adevăr, pentru ca acesta să pară mai plauzibil. Amalgamul rezultat, ce are efectul de a induce în eroare publicul-lint.1 în unele privinţe semnificative, este adesea denumit „dezin-Inimarc” 30.

I»csigur, este posibil ca un mesaj în totalitate adevărat (sau unul i onsiderat adevărat de către cei care îl propagă) să aibă efectul dorit uMipra publicului-ţintă. Fragmentul din discursul lui Hruşciov care a produs cele mai multe efecte (în sensul diminuării prestigiului comunismului în Europa de Vest şi de Est) consta în dezvăluirile legate de «i uncie şi „cultul personalităţii” ale lui Stalin. Publicarea acestuia a irpi czentat o acţiune secretă eficientă a CIA, deşi fragmentul respectiv îl icxtului era indiscutabil autentic. În mod similar, dezvăluirea de «a Ire britanici a telegramei originale a lui Zimmerman, despre care am discutat în capitolul anterior, a fost o lovitură de maestru a ptopagandei ce nu poate fi neatribuită unei anumite entităţi.

Sprijin pentru forţe politice prietene

O altă modalitate de influenţare a evenimentelor din alte ţări catf asigurarea de sprijin material forţelor politice prietene, cum ar A partidele politice, grupurile civice, sindicatele şi presa. Deşi acaat lucru se poate face şi în mod deschis, iar uneori chiar aşa se întâmplă, ajutorul acordat în secret poate părea mai indicat gru parilor beneficiare, de vreme ce astfel este mai puţin probabil i apară acuzaţii privind ingerinţe străine în afacerile interne ale ţării, de natură să

le afecteze pe plan politic.

Desigur, aşa s-a întâmplat în cazul asistenţei acordate în secret de americani sindicatului polonez independent Solidaritatea, în anii ’80 Lucrând împreună cu Biserica Catolică şi cu sindicatele americane, Guvernul Statelor Unite a perfectat un program care viza menţinerea sindicatelor poloneze şi a mişcării democrate poloneze după ei Guvernul comunist al ţării instaurase în decembrie 1981 starea de asediu. Printre tipurile de asistenţă acordată în secret Solidarităţii se numărau fonduri, prese de tipar şi echipament clandestin pentru comunicaţii31.

În mod tradiţional, fosta Uniune Sovietică a facilitat acest tip de activitate făcând o distincţie fictivă între guvernul sovietic şi Partidul Comunist al Uniunii Sovietice. În vreme ce Guvernul putea avea relaţii corecte din punct de vedere diplomatic cu alte state, Partidul, prin intermediul unor organizaţii precum Comintern, Cominform (Biroul Comunist de Informaţii, care din 1947 până în 1956 a transmis „linia de partid” statelor şi partidelor comuniste străine) şi Departamentul Internaţional al Comitetului Central, a menţinut relaţii cu forţele „progresiste” din întreaga lume şi le-a acordat sprijin32. Ca reacţie la activitatea sovietică de acest gen din Europa de Vest postbelică, Statele Unite s-au implicat într-un program ce derula acţiuni secrete de susţinere a grupărilor politice şi culturale democratice şi a sindicatelor33.

În timpul administraţiei lui Harry Truman (la finele anului 1947), reacţia imediată a fost teama

că alegerile din Italia, programate pentru primăvara anului următor, ar putea fi câştigate de comunişti. Pentru a sprijini demersurile propagandistice făţişe ale Statelor Unite, CIA a derulat activităţi în sprijinul partidelor politice

««luministe, cum ar fi asigurarea de sprijin financiar şi de alte tipuri IÉ» MHiiplu, instruire în domeniul tehnicilor folosite în campaniile – liiinic). De asemenea, Agenţia a încercat să influenţeze socialiştii M mm coopereze cu comuniştii. După cum explica Ray Cline, fost 4M* lor adjunct al CIA:

Ai nule lipuri de asistenţă financiară şi tehnică acordate partidelor i iie îi îi democrate sau altor partide necomuni se, precum şi eforturile de am para socialiştii de fronturile unificate dominate de comunişti trebuiau»rt şi deruleze în secret. Liderii partidelor italiene nu îşi puteau permite «A îi lase pe comunişti să obţină dovezi că sunt susţinuţi din afara ţării, ilrnarece astfel s-ar fi redus din indignarea opiniei publice faţă de ilt prudenţa financiară şi politică a Partidului Comunist faţă de Uniunea Sovietică. Prin urmare, CIA a primit însărcinarea de a furniza fondurile ţi asistenţa tehnică necesare obţinerii de voturi şi câştigării alegerilor34.

În urma victoriei electorale a partidelor necomuniste, CIA „a futl înşiruită să propună anumite programe de informare şi alte «puni de natură politică pentru a neutraliza eforturile comuniştilor»îi a şi extinde influenţa politică în Europa Occidentală” 35. După unu preciza Comisia Church, programul rezultat implica „subvenţii pl, nu îi organizaţiile muncitoreşti şi

politice adverse”, care:

aveau ca scop să servească drept alternative la grupările de inspiraţie sovietică sau comunistă. [Se realizau] operaţiuni vaste în domeniul sindical, mediatic şi electoral, la sfârşitul anilor ’40. Sprijinul pentru niganizaţiile „adverse”, în special în activităţile vizând sindicatele, studenţii sau cele culturale, urmau să capete o amploare mult mai mare în anii ’50 şi 6036.

După cum sublinia Ray Cline, majoritatea fondurilor ajungeau la umanizaţii ale stângii necomuniste, care nu susţineau neapărat anumite poziţii ale Statelor Unite în ce priveşte politica externă. El «uează în special Congresul pentru Libertate Culturală şi publicaţii pol îi ice precum *Encounter* din Anglia şi *Der Monat* din Germania de Vest*7. Această strategie se pare că a fost dictată de opinia că pl, meipalul câmp de luptă ideologic al Europei viza forţele de stânga i ea organizaţiile mai conservatoare ar avea, în orice caz, mai puţine hlicultăţi de a obţine fonduri de pe plan intern. Totuşi, ea scoate în vulenţă o ambiguitate tipică acţiunilor secrete: este adesea posibil să lucrezi cu oameni cu care ai divergenţe de opinie majori Problemele pe care le-ar cauza divulgarea unui astfel de aranjament devin un alt motiv pentru păstrarea secretului.

Un program american mai controversat de acest tip a fost apllcü în Chile, după instalarea marxistului Salvador Allende în funcţii dl preşedinte, în 1970. Acest program avea ca scop să asigure partidoluf politice de opoziţie şi presei resursele financiare necesare pentru supravieţui

în contextul haosului economic din ţară şi al măsurilor dl reglementare ostile adoptate de către guvern. Controversa pl, marginea acestui program s-a concentrat asupra a două aspecu (dincolo de întrebarea mai generală vizând ce poziţie ar fi trebuit i adopte SUA faţă de regimul lui Allende).

În primul rând, programul a fost considerat inutil deoareci, conform Comisiei Church, evaluările naţionale de securitate ale CIA din perioada regimului Allende indicau faptul că, „în ciudi încercărilor de a hărţui şi de a afecta din punct de vedere financiar presa de opoziţie", aceasta (şi în special *El Mercurio*, cel mai mari ziar naţional şi cel mai important mijloc de comunicare în masă ci propaga idei defavorabile lui Allende) a rămas liberă, iar „sistemul politic tradiţional din Chile a continuat să manifeste un curaj spectaculos" 38. Totuşi, Comisia a observat că responsabilii cu elaborarea acestor evaluări nu aveau cunoştinţă de programul de acţiuni secrete; „Prin urmare, nu a existat o evaluare care să arate dacă aceste sectoare ar supravieţui *fără* banii proveniţi din SUA"39.

Un alt subiect controversat a vizat scopurile pentru care Statele Unite au acordat acest ajutor. SUA au încercat în mod serios să nu acorde asistenţă acelor grupări care încercau în mod activ să răstoarne Guvernul (cum ar fi sindicatul şoferilor de camioane, întrucât grevele prelungite şi pagubele cauzate ofereau ocazii pentru lovituri militare) şi să-şi limiteze ajutorul acordat la partidele de opoziţie şi la presă. Potrivit lui Gregory Treverton, un critic al acţiunilor secrete

ce era membru al Comisiei Church, „tiparul consfătuirilor din cadrul Guvernului american sugerează o distincţie clară între sprijinirea forţelor de opoziţie şi finanţarea grupărilor care încearcă să promoveze o lovitură militară. Încercarea de stabilire a acestei distincţii a fost, din câte îmi dau seama, un demers onest” 40. Cu toate acestea, după cum conchide şi Treverton, această distincţie era una eminamente artificială, care exista „numai în minţile

Hfcetii miilor, nu şi ale chilienilor” 41. Grupările de opoziţie îşi aleg un-mi strategiile pentru a-şi atinge obiectivele şi îşi selectează tfritt ilr şi aliaţii în consecinţă; dacă diversele forţe adversare lui aluniiiloreau să coopereze, sprijinul Statelor Unite pentru unele Uium* grupări ajungea şi la aliaţii acestora.

hiflunnţarea evenimentelor politice f-iin mijloace violente lu’ în hii opiniei publice, acţiunile secrete sunt adesea asociate mijloacelor, inimile* de influenţare a evenimentelor politice. După cum au demoni Mi în alimentele prezentate anterior, multe tehnici nonviolente pot în unii/ale în secret pentru a se influenţa comportamentul politic, rumentele şi situaţia din alte ţări. Dar, în plus faţă de aceste le tiv unii ce reprezintă majoritatea tipurilor de operaţiuni secrete, Minin şi tehnici care implică susţinerea sau utilizarea violenţei.

*Sprijinirea loviturilor de stat*, *„războaiele de eliberare naţională99* şi *„luptătorii pentru libertate99*. Sprijinul acordat grupărilor politice nu îi rhu le să se limiteze la oponenţii paşnici ai unui guvern străin, i poate fi extins asupra

grupărilor care încearcă fie să influenţeze i m. 111 a a guvernului respectiv prin mijloace violente, fie să îl răstoarne. Ansi lucru poate implica sprijinirea unei grupări existente sau i o ai ea unei grupări-„marionetă”, care să realizeze aceste activităţi42, lipul exact de sprijin acordat depinde parţial de gruparea m şi nu/a şi de strategia adoptată de aceasta. El poate lua forma asistenţei militare acordate forţelor combatante insurgente, a sprijinului operaţional în cazul loviturilor de stat, a presiunilor politice şi economice im ne sau a actelor subversive interne îndreptate împotriva guvernelor

* i/ale de asemenea, se poate acorda sprijin economic sau constând în instruire pentru dezvoltarea cadrului unor lupte de gherilă de liiujtf durată. Un exemplu în acest sens îl reprezintă cele două mari îi put i se acţiuni secrete cunoscute, în principiu, puse în practică de Matele Unite în timpul administraţiilor lui Jimmy Carter şi Ronald Uragan (sprijinul pentru luptele de gherilă împotriva regimului afgan aistinut de sovietici şi sprijinul acordat contrarezistenţei în Nicaragua).

O formă deosebită a acestui tip de activităţi căreia i s-a acordat multă atenţie este sprijinul acordat de un stat-sponsor terorismului internaţional. Sprijinul pe care îl acordă guvernele grupărilor terotl Ms poate diferi mult în ce priveşte amploarea şi semnificaţia. La Îiimh inferioară, un stat-sponsor poate asigura facilităţi de instruire aH adăpost unde teroriştii să fie în siguranţă, unde să nu poată fi are Miţi. În timp ce

îşi pregătesc atacurile sau unde să fugă ulterior. La Îiiniu superioară, acest sprijin poate include fonduri, arme, paşapoarH autentice sau false ori utilizarea curierilor diplomatici pentru trai» miterea unor arme sau explozibili în ţara vizată. Şi nivelul controlului exercitat de statul-sponsor asupra activităţilor grupării teroriste poatl varia; în unele cazuri acesta poate fi destul de strict, în vreme ce tfl alte cazuri poate să nu existe, câtă vreme natura generală a activităţilen corespunde intereselor statului-sponsor.

*Forţele paramilitare*. La limita dintre adevăratele acţiuni secreU şi acţiunile militare se află cazurile în care un guvern foloseşte trupa clandestine (sau voluntari) într-un conflict militar, fie de sine stătătoam, fie în alianţă cu grupări similare sau cu trupe locale. Deoarece un demers de acest gen la scară largă poate cu greu să fie ţinut secret mult timp, putem considera că acest tip de activitate ar trebui exclu* din categoria acţiunilor secrete. În schimb, de vreme ce este probabil ca serviciile de informaţii să primească misiuni de acest gen, tla obicei aceste acţiuni sunt asociate cu alte tipuri de activităţi secrete Totuşi, din moment ce activitatea nu va fi recunoscută public da către guvernul care o coordonează, ea rămâne secretă din accul punct de vedere, indiferent de cât de transparentă devine pretenţia de neimplicare.

*Acte specifice de distrugere sau violenţă, inclusiv asasinaţi*, Acţiunile sub acoperire pot lua forma anumitor acte de violent, îndreptate împotriva unor persoane (cum ar fi asasinarea

reprezen tanţilor guvernelor străine, a unor figuri politice emblematice sau a teroriştilor) sau a unor bunuri.

*Wet affairs* (eufemism pentru asasinat şi sabotaj) au fost, în diverse momente, un element obişnuit al operaţiunilor serviciilor sovietice de informaţii. Probabil cel mai cunoscut eveniment de acest gen a fost uciderea lui Leon Troţki în Mexic, în 1940. În Statele Unite, încercările eşuate ale CIA de a-l asasina pe Fidel Castro, precum şi colaborarea acestei agenţii cu forţele politice

(twi Mduhile de asasinarea lui Patrice Lumumba din Congo şi a lui piM lïujillo din Republica Dominicană au fost printre cele mai utif MIH iinir chestiuni care au ieşit la iveală în timpul anchetelor A»Mitiri de la jumătatea anilor ’70, fiind atent studiate de către IHnmnlii („hurch43. Un rezultat al acestor dezvăluiri a fost includerea şi ţi-l relui privind activitatea de informaţii al preşedintelui Gerald ml inie impunea o interdicţie explicită asupra „implicării sau Mttplinrii în vederea implicării în asasinate politice” 44. Această imt cine a fost menţinută în decretele privind activitatea de iiifonnalii ale preşedinţilor Carter şi Reagan45. Chestiunea în cauză i (nul adusă din nou în atenţia publică la finele anilor ’80, în legătură în politica Statelor Unite în ce-l priveşte pe proeminentul om politic lua Panamá Manuel Noriega, când s-a susţinut că prevederea huplmlica CIA să le acorde asistenţă membrilor organizaţiei care i se upmira lui Noriega, Forţa de Apărare din Panamá, pentru plani hi arca unei

lovituri de stat (deoarece acest lucru ar fi putut să simplu e asasinarea lui Noriega sau să ducă la acest rezultat) 46. Din

* pe (punct de vedere, prevederea a contribuit, prin urmare, în mod liwlticcl la invadarea de către SUA a statului Panamá în decembrie IUHM, ceea ce a dus la destituirea lui Noriega, dar cu un preţ mult mul mare.

Una dintre acţiunile secrete mai bine cunoscute care a implicat tininilp la adresa proprietăţilor a fost aruncarea în aer de către ftgiuilii francezi de informaţii a vasului *Rainbow Warrior*, în 1985. Ai castă navă, care a fost atacată în timp ce se afla în port în Noua / Handă, aparţinea organizaţiei de protecţie a mediului Greenpeace.

*p* intenţiona să o folosească pentru a protesta faţă de testele cu arme «iiituice derulate de Franţa în Pacificul de Sud şi pentru a încerca împiedicarea acestora. Un fotograf portughez aflat la bord a fost ucis Im greşeală în explozie.

Un exemplu de activitate mai distructivă de acest tip a fost atupania germană secretă de sabotaj care a avut loc în Statele Unite înainte ca acestea să ia decizia de a se implica în Primul Război Mondial. Deşi poziţia lor oficială era neutră, Statele Unite au fost le iuşi un furnizor important de muniţii şi materiale de război pentru Marea Britanie şi aliaţii acesteia în primii trei ani de conflict. Pentru a întrerupe acest flux de materiale către adversarii săi – fără a genera i reacţie a Americii îndreptată împotriva Germaniei – serviciile germane de informaţii au realizat

multe operaţiuni secrete în Sln»l» Unite. Printre acestea se numărau sabotarea vaselor care transport” provizii în Marea Britanie şi Rusia, producerea unor viruşi de am «care să fie injectaţi cailor şi măgarilor trimişi în Europa şi bombat darea fabricilor de muniţie şi explozibili aflate pe Coasta de Est. Cai mai spectaculoasă acţiune a fost sabotarea căii ferate şi a terminalului maritim de la Black Tom, din New Jersey, în iulie 1916. Foloaliul dispozitive de incendiere şi explozibili, agenţii germani au distrui complet locul şi, împreună cu el, o cantitate impresionantă de muniţii destinate războiului din Europa. Distrugerea terminalului, poziţional transversal faţă de Statuia Libertăţii, a zguduit Brooklyn Bridgo, spulberat ferestrele în întregul Manhattan şi a putut fi auzită chiar din Philadelphia47.

Acţiunile secrete şi păstrarea confidenţialităţii

Deşi caracterul secret pare a sta la baza acţiunilor secrete, importanţa şi funcţiile sale, după cum s-a menţionat la începutul acestui capitol, nu sunt deloc chestiuni simple; ele depind foarte mult de tipul da acţiune secretă şi de împrejurările în care este ea asumată. Gradul da secretizare necesar şi motivarea acestuia pot diferi foarte mult de la caz la caz.

În unele situaţii, păstrarea secretului poate fi absolut vitală pentru succesul operaţiunii. De exemplu, amiralul Stansfield Turner, director al CIA în timpul preşedintelui Carter, a prezentat o ope raţiune care implica trimiterea unui agent CIA la Teheran pentru a facilita eliberarea a şase

americani ce se refugiaseră în Ambasada Canadei, după ce se pusese sechestru asupra Ambasadei Americane, în noiembrie 197948. Orice dezvăluire privind operaţiunea (chiar dacă identitatea agentului CIA şi a celor şase persoane care se ascundeau nu ar fi fost dată în vileag) ar fi pus în pericol siguranţa celor şapte oameni implicaţi, atrăgând atenţia iranienilor, determinându-i pe aceştia să intre în Ambasada Canadei sau complicând procesul de scoatere a americanilor din Iran cu ajutorul unor paşa poarte false.

Im iimhl asemănător, păstrarea secretului asupra unor detalii ale «i ihialiuni poate fi necesară pentru a împiedica apariţia unor 4 mr nir în calea acesteia, chiar dacă elementele generale ale prompthiiiliii sunt cunoscute. Să luăm ca exemplu programul Statelor!» de asistenţă pentru rezistenţa *mujahedinilor* împotriva Uniunii le»MNR în Afganistan, din anii ’80. Au existat mai multe ţări şi

«! specifice prin intermediul cărora se transmiteau ajutoare IMIH iiiri; dacă acestea ar fi fost făcute publice la momentul *«în iiv, ar fi fost vulnerabile în faţa presiunilor diplomatice sau a MM-iiliii din partea guvernului sovietic sau a celui afgan49. Prin ruMMir, în ceea ce priveşte detaliile operaţiunilor secrete, este t»t’ MIA păstrarea secretului, indiferent cât de promovată este ope

.» im *a* în general.

AMiel de cazuri, în care secretul întregii operaţiuni sau a unor unic aspecte ale sale este esenţial pentru ducerea ei la bun sfârşit.

(! lui ci sunt rare. Totuşi, în multe alte situaţii

confidenţialitatea mii h urle importantă pentru asigurarea eficienţei operaţiunii. În i i.i categorie considerăm că se încadrează tipurile de propagandă tu nu poate fi atribuită unei entităţi sau sprijinul acordat actinulilor politice, ce au fost discutate anterior.

Ai este activităţi sunt realizate în secret deoarece transmiterea»lui opinia publică de informaţii referitoare la sursa externă a i paf, aiidei sau a fondurilor pentru acţiunile de natură politică le-ar mina efectul. De exemplu, conceptul de *propagandă „neagră”* în Metmiia că informaţiile ce ar fi puse sub semnul întrebării sau… i mi isc dacă s-ar şti că provin dintr-o sursă a adversarilor sau luni o sursă externă şi care are un motiv ascuns evident ar fi mai vu «le acceptat dacă originea lor ar putea fi ascunsă sau dacă ele ar fi.m limite altcuiva. (în multe situaţii, păstrarea secretului ar fi sară şi pentru că finanţarea organizaţiilor politice ar încălca lirile (arii vizate).

În plus, propaganda „neagră” poate fi folosită pentru a crea îi misiuni în rândul oponenţilor, prin atribuirea în mod fals a unor I«Iu am sau acţiuni provocatoare. În acest caz, nedivulgarea ade Ai alei surse a propagandei este necesară pentru a i se menţine iiilihilitatea. Sefton Delmer, care a condus operaţiunile britanice ilr uopagandă „neagră” în timpul celui de-al Doilea Război Mondial, m.linca că „propaganda cea mai simplă şi mai eficientă este să în lupi în supa cuiva şi apoi să strigi *Heil Hitler” 50*. De asemenea, multe dintre documentele produse de fosta Uniune Sovietic* tun false memorandumuri ale Guvernului

american care demonstrau atitudine ostilă faţă de un terţ stat.

În alte situaţii, păstrarea confidenţialităţii poate fi necesară peiun a se asigura cooperarea unei terţe părţi care este dispusă să îşi i»I. «ajutorul numai dacă activitatea este secretă, pentru a evita sit cu deterioreze relaţiile externe. Din acest motiv, chiar şi în cazurile *k* care elementele generale ale unei activităţi secrete pot fi *tttM* publice fără probleme, păstrarea secretului privind aceste activus poate fi importantă.

O altă categorie vizează cazurile în care se evită informării publicului nu pentru că aceasta i-ar pune în pericol pe cel realizează operaţiunea sau pentru că i-ar reduce eficienţa, ci pentru că motive diplomatice fac să se prefere nerecunoaşterea implielttt guvernului51. De exemplu, nerecunoaşterea oficială a unei operaţiuni poate împiedica reacţia unui adversar, chiar dacă acesta deţine (Im» de la serviciile de informaţii privind implicarea. Acest lucru oid valabil în special dacă adversarul este o democraţie în care guvernul trebuie să obţină sprijinul sau înţelegerea publicului pentru orlu reacţie pe care ar putea să o aibă. Adversarul poate fi împiedicat»! încerce să obţină sprijinul public de teama că prezentarea dovezii», incriminatoare ar pune în pericol mijloacele cu ajutorul cărora în fost culese. Prin urmare, este firesc ca un stat care sprijină terorismul internaţional să nege că ar avea orice legătură cu un anumit ev* nimeni de natură teroristă, deşi complicitatea sa devine cunoscut!

De exemplu, capacitatea Guvernului american de a reacţiona li atacurile teroriste cu bombă atribuite Libiei, din 9 aprilie 1986, asupra unei discoteci din Berlinul de Vest, în care un militar arne* rican şi o altă persoană au fost ucişi, depindea în mod esenţial di disponibilitatea Statelor Unite de a divulga date obţinute de li serviciile de informaţii care dovedeau implicarea Libiei. Deşi Guvernul Statelor Unite a procedat astfel, a plătit un preţ mare; libienii au luat cunoştinţă de dimensiunile capacităţilor informative americane îndreptate împotriva lor şi, prin urmare, au reuşit să le reduci eficienţa52.

În general, deşi se subînţelege că guvernele se implică în acţiuni secrete (deoarece se implică în spionaj), acestea sunt de multe oii ilegale conform legislaţiei ţării pe teritoriul căreia se desfăşoară. De

…»mă, ele pot fi şi contrare legilor internaţionale, la baza cărora ni h«me ipuil neintervenţiei în afacerile interne ale statelor suverane, 1*91 mesi principiu are din ce în ce mai puţină greutate în ihiiiţiii Mlen (a internaţională după încheierea Războiului Rece53.

I mm în este motive, la nivelul relaţiilor diplomatice este preferabil d mm le recunoască o operaţiune, chiar dacă ţara ce are de suferit de *r* mi mim ei are cunoştinţă despre implicarea celeilalte. Ţara vizată peu înnora acţiunile secrete, fie în interesul păstrării unor bune Uţii l ic pentru că nu le poate împiedica; este însă mult mai dificil pumni ea să procedeze astfel dacă guvernul care o conduce îşi intimste public atitudinea.

— MMNI plauzibilă

M.«luna considerată multă vreme axiomatică potrivit căreia, chiar 4* ɪ\ implicarea unui stat într-o acţiune secretă devine cunoscută, – ml de stat ar trebui să poată nega că a autorizat sau chiar că a avut niMoiiiuţă despre ea este strâns legată de cele menţionate anterior. 4. i Nu ar trebui să poată afirma, destul de plauzibil, că operaţiunea 4 f»mi îndeplinită de subordonaţi ai săi care au acţionat fără ştirea ori «»iie în zarea lui.

În perioada postbelică, această doctrină a intrat în atenţia publică i în h i când, după cum s-a menţionat, preşedintele Eisenhower nu a unui seama de ea şi a recunoscut public că autorizase survolarea i uit nu-i Sovietice cu aeronava de recunoaştere U-2. Reacţia lui i e.niliower a avut loc în mai 1960, după ce un avion U-2, anterior im nincrabil la atacuri ale forţelor de apărare aeriană datorită altitudinii MMI i la care zbura, a fost doborât de o rachetă sol-aer a sovieticilor în iiinp ce se afla într-un zbor de recunoaştere deasupra teritoriului km (Deşi nu era vorba despre o acţiune secretă, acest incident, ce implica o aparentă încălcare a prevederilor legislaţiei internaţionale», iulicat aceeaşi problemă a negării plauzibile.)

Iu biografia sa, prim-secretarul sovietic din perioada respectivă, Nikita Hruşciov, urma să susţină că asumarea răspunderii de către i i «nhower, şi nu zborul în sine l-a determinat să grăbească întâlnirea i «nivel înalt de la Paris a „celor patru”, programată să aibă loc mai iai/.în, în acea primăvară54.Totuşi, Eisenhower a considerat că nu [ţuica să nege că ştia, fără a

insinua că nu controlează eficient forţele militare americane, dată fiind infrastructura amplă necesară sun (Îi»i zborurilor. Deşi este posibilă negarea operaţiunilor unui grup miitip agenţi secreţi, care poate fi descris ca fiind format din trădăloil te acţionează împotriva ordinelor sau fără ordine, tăgăduirea unei oif raţiuni care implica evident cooperarea multor persoane din diviM baze aviatice din toată lumea este cu totul altceva.

Un exemplu de negare plauzibilă din ultimii ani este emul agenţilor francezi de informaţii care au aruncat în aer vasul *Rainbm Warrior*. Când ofiţerii francezi de informaţii implicaţi au fost arculur în Noua Zeelandă, a devenit evident cui îi revine responsabiliul H pentru această situaţie. Guvernul francez a susţinut că implicufH oficială în această situaţie nu a fost la nivel mai înalt dec Al ministrului Apărării, Charles Hernu, care răspundea de D0 (Direction Générale de la Sécurité Extérieure, serviciul francez de informaţii externe, subordonat Ministerului Apărării). Acesta a demi sionat la trei luni după atacuri. Preşedintele François Mitterrand l scăpat aproape neatins55.

În Statele Unite, doctrina negării plauzibile a fost în fapt abollll de Congres în urma investigaţiilor asupra chestiunilor legate de serviciile de informaţii de la jumătatea anilor ’70. La sfârşitul anului 1974, în urma dezvăluirilor despre un program de acţiuni secrete în Chile, Congresul a aprobat Amendamentul Hughes-Ryan, cart interzicea CIA acţiunile derulate în secret:

…în afara situaţiilor în care preşedintele constată că fiecare operaţiuni în parte este importantă pentru securitatea naţională a Statelor Unite l informează în timp util… comisiile responsabile ale Congresului, inclusiv [Comisia pentru Relaţii Externe a Senatului şi Comisia pentru Afaceri Externe a Camerei Reprezentanţilor]56.

Atenţia acordată de Congres Amendamentului s-a axat pe componenta acestuia care solicita puterii executive să informeze Congresul asupra acţiunilor secrete. Totuşi, prevederea Amendamentului conform căreia preşedintele trebuie să constate că acţiunile secrete propuse sunt importante pentru securitatea naţională a subminat capacitatea preşedintelui de a nega plauzibil implicarea în orice acţiune sub acoperire care era adusă în atenţia publicului57.

În cursul anchetei Iran-Contra, afirmaţiile amiralului John Pointdexter conform cărora nu l-ar fi informat pe preşedintele Reagan despre

«mii lui veniturilor obţinute din vânzarea armelor iraniene către 11*11 mă din Nicaragua au reprezentat o încercare de resuscitare a é* li luci negării plauzibile. Mai exact, Pointdexter a depus mărturie fi nu I a informat pe preşedinte despre transferurile de fonduri… nu.1 i asigura acestuia „posibilitatea de a nega ulterior imbr-iţiile. În caz că ele ar fi făcute publice” 58.

Năiiunţarea la confidenţialitate

Mm muza rolului tot mai important al Congresului în controlarea i Hunilor secrete,

Statele Unite au renunţat, de fapt, în ultimii în la confidenţialitate în cazul unor operaţiuni care, în mod normal, ar fi denumite (şi încă mai sunt denumite, adesea) acţiuni wiric. De exemplu, chestiunea ajutorului acordat insurgenţilor im Alganistan şi Nicaragua a fost discutată deschis şi dezbătută în i iMUiies şi în presă. Statele Unite chiar şi-au susţinut, în acordul de u «irneva din 1988 privind retragerea sovieticilor din Afganistan, în inul de a continua să le acorde asistenţă rebelilor, câtă vreme iitviriicii ajutau Guvernul de la Kabul. Deşi aceste activităţi erau numite acţiuni secrete, ele nu erau astfel din multe puncte de vedere. În uncie cazuri, Congresul a preluat în mod deschis iniţiativa de a în opune acţiuni, cum ar fi asigurarea de sprijin forţelor irakiene ce cu opuneau regimului lui Saddam Hussein, care în trecut ar fi fost i Miisulerate acţiuni secrete59.

În alte cazuri, Statele Unite au renunţat complet la confiden-li, iliiatea acţiunilor despre care s-ar fi considerat, anterior, că o impun. În 1973, de exemplu, după ce s-a confirmat public că CIA i manta *Radio Europa Liberă*/*Radio Libertatea* (RFE/RL), Congresul» înlocuit mecanismul de furnizare a fondurilor în secret cu finanţarea iMivernamentală deschisă prin intermediul unei agenţii guvernamen-i.ilc independente nou-create, Comitetul pentru Radiodifuziune h aci naţională. Deşi această schimbare nu a fost realizată voluntar, ac posibil să nu fi avut un efect considerabil asupra credibilităţii Klii/RL în ţările vizate. Dacă la început ascunderea surselor de

nuanţare este posibil să fi sporit eficienţa RFE/RL, se pare că în 1 J73 posturile de radio aveau deja o serie de realizări pe baza cărora I uiteau fi judecate de către opinia publică.

În mod similar, în urma discursului preşedintelui Reagan de li Londra din 8 iunie 1982, în care acesta cerea consolidarea infrastructuiU democraţiei la nivel global, a fost înfiinţată organizaţia privată tu finanţare federală Naţional Endowment for Democracy, în anul 19H1 Aceasta oferă sprijin nedisimulat (direct şi prin intermediul instituţilliif afiliate AFL-CIO*, Camerei Americane de Comerţ şi partidelut Democrat şi Republican) instituţiilor – sindicate, asociaţii ale oamenilt* de afaceri, alte organizaţii civice, presă şi partide politice – citit promovează democratizarea sau contribuie la consolidarea denw craţiei în ţările unde ea este precară, ameninţată ori inexistentă60.

Acest demers a fost, într-o oarecare măsură, realizat după modelul activităţilor internaţionale ale fundaţiilor politice asociate partidelor politice vest-germane61; aceste fundaţii sunt finanţate de către Guver* nul german şi funcţionează prin intermediul unor organizaţii poliţiei cu viziuni similare din alte ţări care au ca scop promovare! democraţiei. În general, se consideră că acestea au acordat sprijin, spre exemplu, partidelor necomuniste din Portugalia, în perioadl tulbure şi periculoasă ce a urmat înlăturării dictaturii lui Caetano”, în 1974. Din anumite puncte de vedere, acest tip de sprijin fă-ţi acordat instituţiilor democratice a substituit parţial ajutorul acordai

de Statele Unite în secret forţelor democratice din Europa de Voal imediat după al Doilea Război Mondial.

Acţiunile secrete şi activitatea de informaţii

După ce am trecut în revistă gama variată de activităţi care se încadrează în categoria acţiunilor secrete, vom analiza relaţia dintre acestea şi restul activităţilor de informaţii. Se ridică două întrebări. Prima: ar trebui ca acţiunile secrete să fi realizate de către agenţiile care culeg informaţii şi le analizează sau să fie integrate într-o structură birocratică separată? A doua: din perspectivă pur teoretică, acţiunile secrete ar trebui să fie considerate parte integrantă a activităţii de informaţii?

— American Fédération of Labor and Congress of Industrial Organizations – cea mai mare federaţie sindicală din Statele Unite (n.r.).

** Marcello Caetano – şeful Guvernului portughez care i-a succedat lui Salazar, în perioada 1968 – 1974, până la Revoluţia Garoafelor din 1974 (n.r.).

*h* Irabui ca acţiunile secrete să fie independente?

*I»innn /de împotriva existenţei unei agenţii independente pentru* cu *Hum secrete*. După cum am precizat în primul capitol, atât Statele lmiu\ eftt şi Marea Britanie au descoperit empiric faptul că existenta i ilimia organizaţii implicate în operaţiuni clandestine – una pentru i mivjmm ca informaţiilor (spionaj) şi una pentru acţiuni secrete – poate»m probleme importante de ordin practic. În timpului celui de-al iMlra Război

Mondial, SOE (British Special Operations Executive),» «nmu/iitia abilitată de prim-ministrul Winston Churchill „să arunce luunpa în aer”, a fost separată de Serviciul Secret de Informaţii (SIS nu M16) şi subordonată ministrului pentru Războiul Economic. MHH au luat naştere inevitabilele rivalităţi interdepartamentale, avnarece ambele agenţii se luptau pentru aceleaşi resurse limitate62.

În mod similar, în Statele Unite o componentă specială a CIA, umilită Oficiul pentru Coordonarea Strategiilor (Office of Policy i iMudination – OPC), a fost înfiinţată în 1948 pentru a realiza 4 i plini secrete. Deşi, din punct de vedere administrativ, făcea parte»Hu CIA, Oficiul acţiona pe baza indicaţiilor de strategie primite de M I apartamentul de Stat şi Departamentul Apărării, iar conducătorul au n-a numit de secretarul de stat63. Acest Oficiu a fost separat de Oficiul I«uhu Operaţiuni Speciale (Office of Special Operations – OSO) al MA, care culegea informaţii prin activităţi de spionaj. În cele din în mă, acest sistem s-a dovedit a nu fi eficient, iar cele două oficii au h»hi integrate în 1952 în nou-înfiinţatul Directorat pentru Planificare64, h»li ivit Comisiei Church, această măsură a fost determinată de: 1) l»4 t/i (la nefirească în care se afla directorul CIA, ce avea un oficiu impi) pentru care era responsabil din punct de vedere administrativ i) i care era finanţat prin intermediul CIA), dar care primea instrucţii direct de la Departamentul de Stat şi Departamentul Apa rării; 2) competiţia dintre OPC ŞI OSO pentru serviciile aceloraşi îi iuţi şi, dată

fiind rivalitatea, dificultăţile asigurării unei cooperări irperative între acestea, atunci când era necesar65.

Deşi teoretic funcţiile lor sunt diferite, acţiunile secrete şi cule – «ca informaţiilor din surse umane se bazează pe mijloace similare, în special pe cooperarea secretă dintre agenţii capabili să opereze «licient în ţara vizată. În multe cazuri, agenţii care ar fi utili pentru realizarea uneia dintre funcţii o pot îndeplini şi pe cealaltă. Se unui§ întâmpla foarte uşor ca două oficii separate să concureze prim serviciile aceloraşi persoane. În plus, multe dintre funcţiile adiaceirtf cum ar fi asigurarea comunicaţiilor între ofiţeri şi agenţi sau efectuam plăţilor clandestine, sunt asemănătoare sau identice şi necesită abilitat) contacte şi resurse similare. Este necesară coordonarea strictă pornii a se evita ca operaţiunile unui oficiu dintr-o anumită ţară «Ale afecteze pe cele ale celuilalt. O astfel de coordonare poate fi greu th realizat, în special dacă ar impune ca interesele unui oficiu şi la subordonate intereselor celuilalt. Prin urmare, există argumonH puternice în favoarea integrării acestor funcţii într-o singură organi/afli ale cărei operaţiuni în ţara sau regiunea vizată să fie controlate de UA singur şef.

*Argumente în favoarea existenţei unei agenţii independenţi pentru desfăşurarea de acţiuni secrete*. Deşi, din punct de vedon operativ, ar fi preferabilă consolidarea acestor funcţii, s-a susţinut el natura diferită a sarcinilor implicate face ca ea să nu fie indicată. S-i adus în special

argumentul că, acordând aceleiaşi organizaţii, pe il* o parte, responsabilitatea pentru implementarea politicilor (prin acţiuni secrete) cu privire la o anumită ţară şi, pe de altă parte, sarcina de culegere şi analizare a informaţiilor cu privire la acea (ari (inclusiv de evaluare a rezultatelor acţiunilor secrete), se pune în pericol obiectivitatea analizei. În principiu, acesta este acelaşi argument care a fost adus în favoarea înfiinţării unei agenţii centrale de informaţii – şi anume ca aceasta să nu facă parte dintr-un ministet sau departament al guvernului care trasează ori implementeazfl strategii.

Acţiunile secrete fac parte din activitatea de informaţii?

Lăsând la o parte aspectul organizatoric, rămâne întrebarea teoretică dacă acţiunile secrete trebuie considerate parte integrantă a activităţii de informaţii. Incluzând acţiunile secrete în rândul elementelor activităţii de informaţii, am subliniat că aceasta este o funcţie caracteristică a agenţiilor de informaţii; acest fapt în sine nu răspunde

(M liiieh, lrii dacă este firesc ca, teoretic, să le considerăm parte a.«ni! du informaţii”.

h»uiru a răspunde acestei întrebări, e nevoie să înţelegem mai tot* r sunt acţiunile secrete. După cum am precizat deja, termenul h tiu» este preluat din vocabularul specific serviciilor de informaţii téu. M ia. Şi nu are echivalente clare în uzul curent al serviciilor de i., în u (îi din alte ţări. În plus, diversele definiţii ce i s-au dat în 1 A au survenit în contextul încercărilor de reglementare

a acţiunilor inc prin lege sau prin decret; ele nu sunt neapărat utile pentru h»i nucii de faţă.

ţinând în revistă tipurile de acţiuni secrete, unele (cum ar fi ipuul acordat în secret unui regim prieten) par aproape imposibil t. icparat de diplomaţie, în timp ce altele (cum ar fi activitatea (HUiuuilitară) se transformă treptat în lupte de gherilă sau războaie li imensitate redusă". Ceea ce pare a fi exclusiv acţiune secretă r cu i alea de mijloc dintre diplomaţie şi război ce implică manipularea im icnet a percepţiilor celorlalţi, pentru a-i determina să ia măsuri p. are cineva le consideră în interesul său. Prin urmare, fac parte în (lunile secrete din activitatea de informaţii?

IV de o parte, s-a susţinut că acţiunile secrete – mijloace de implementare a strategiilor – sunt foarte diferite de restul activităţii în informaţii, care se ocupă de obţinerea datelor pe care trebuie să în ki/.eze strategiile, fiind, prin urmare, o greşeală ca ele să fie Hiusiderate parte a activităţii de informaţii. Din acest punct de miere, acest tip de activităţi sunt clasificate mai rezonabil drept unul dintre numeroasele instrumente de politică externă – cum sunt, hplomaţia, ajutorul economic, statutul comercial de „naţiunea cea mai favorizată", propaganda făţişă, programele de colaborare, programele de tipul Peace Corps, diplomaţia publică, asistenţa militară şi ameninţarea cu utilizarea forţei militare sau folosirea efectivă *am* csieia – pe care o naţiune le foloseşte pentru a-şi promova interesele67.

Pe de altă parte, cele de mai sus pot fi contestate cu argumentul i-a definirea activităţii

de informaţii drept activitate care vizează ni» (inerea anumitor date este prea limitată: dacă obţinerea informaţiilor este atât de importantă, şi ascunderea datelor valoroase faţă i le adversari trebuie să constituie o componentă importantă a activităţii de informaţii. După cum se va arăta clar în capitolul următor, o modalitate eficientă şi deosebit de profitabilă de a împiedica adversarii să afle adevărul este să îi convingi să creadă o minciună. Din.» «– perspectivă, acţiunile secrete şi contraspionajul prezintă asem Atttfi importante. Cel mai important, ambele pot implica influen (iM«t comportamentului adversarului prin manipularea percepţiilor acomun întrebarea dacă acţiunile secrete fac parte din activitatea de informaţii este strâns legată de modalitatea de definire a ace»t«li Această chestiune va fi reluată în capitolele finale ale cărţii.

Capitolul 5

Spion contra spion: activitatea de contrainformaţii

I Mutre toate ramurile activităţii de informaţii, activitatea de loiirtiâiformaţii este, probabil, cel mai greu de definit. În linii mari, niuhilormaţiile se referă la datele culese şi analizate, precum şi la ijh hiiitmile întreprinse pentru a proteja un stat (inclusiv activităţile i.»m, inimi serviciu de informaţii) împotriva atacurilor venite din m»am serviciilor de informaţii adverse. Conform acestei definiţii», iivitatea de contrainformaţii are aceleaşi obiective ca şi cea de hihiimaţii în sine, de vreme ce trebuie să preîntâmpine orice fel de * (luni ale serviciilor de

informaţii adverse1. Totuşi, într-un sens mai în mi aus, activitatea de contrainformaţii se referă de cele mai multe, ui în riet la prevenirea culegerii de informaţii de către un serviciu divers, fapt ce i-ar oferi un avantaj. Vom studia mai întâi conceptul le *activitate de contminformaţii*.

l’entra a înţelege ce implică prevenirea culegerii anumitor inh»imaţii de către un serviciu advers, trebuie să facem mai întâi de huite distincţia între măsuri active şi măsuri pasive. Cele mai importante măsuri pasive, ce au drept scop împiedicarea adversarului nfl culeagă informaţiile dorite, pur şi simplu prin blocarea accesului uiu la acestea – construind un zid în jurul lor –, poartă de obicei Icnumirea „măsuri de securitate” 2. Despre natura acestui zid – împiedicarea accesului la informaţii unor persoane care nu sunt de încredere, protejarea documentelor şi comunicaţiilor prin criptare şi ilepozitarea în locuri sigure etc. – vom discuta în secţiunea despre securitate. Totuşi, în primul rând, guvernul, precum şi diversele sale «Icpartamente şi agenţii trebuie să hotărască ce informaţii sunt suficient de importante pentru a fi protejate – ce informaţii ni intimi te în interiorul zidului.

Clasificarea informaţiilor

Nivelurile de clasificare

Informaţiile sunt clasificate în funcţie de importanţa lor, adică Im funcţie de pericolul pe care l-ar putea reprezenta dezvăluirea Im unei puteri adverse şi, ca urmare, importanţa protejării acestora \\ Statele Unite, primul sistem de

protecţie a documentelor privind securitatea naţională a fost implementat de Departamentul de Răzixil în 1912; Departamentul de Război şi cel Naval şi-au alcătuit propriii» sisteme de clasificare în timpul celor două războaie mondiale1 Preşedintele Harry Truman a pus bazele primului sistem de sificare a informaţiilor la nivel guvernamental în 19514. Sistemul actual este reglementat printr-un decret promulgat de preşedintele Clinton în 1995, care stabileşte definiţii, reguli şi procedună.

*Importanţa informaţiilor* Sistemul de clasificare din Statele Unite încearcă să clasifice informaţiile în funcţie de gradul de atingere îl securităţii naţionale care ar putea fi adusă prin dezvăluirea neautorizată a acestora. Cu cât informaţia este mai importantă, cu atât mai atent trebuie protejată, iar persoanele care beneficiază de „acces" trebuie să fie cât mai puţine. În cadrul sistemului actual, nivelurile de clasificare sunt următoarele: Secret, Strict Secret şi Strict Secret de Importanţă Deosebită, stabilite în funcţie de daunele pe care dezvăluirea neautorizată a acestora l-ar putea aduce securităţii naţionale:

Strict Secret de Importanţă Deosebită: „daune foarte grave";

Strict Secret: „daune grave";

Secret: „daune" 6.

În plus, sunt folosite multe alte prevederi pentru a restricţiona accesul la informaţii. În ceea ce priveşte problemele de securitate, acestea se referă la informaţiile privind tehnicile şi resursele de culegere a informaţiilor secrete; ele sunt

stabilite de directorul CIA trth în conformitate cu atribuţiile sale, reglementate de Legea MMMĂ tli naţionale din 1947, de „protejare a surselor şi metodelor în mm» împotriva dezvăluirii neautorizate” 7. Totuşi, odată cu trecerea Mi»t ai este clasificări (sau „compajtimentări”) speciale s-au înmulţit, «r entităţi atât din interiorul, cât şi din exteriorul comunităţii *é* Indumaţii au încercat să protejeze informaţiile considerate de o ftttptiiian («1 deosebită. Periodic, se încearcă sistematizarea şi contro-fefM ut csiui sistem; cel mai recent decret, de exemplu, prevede ca»tittfiml programelor de acces special să fie menţinut la „un minimhi absolut”, acestea fiind monitorizate de cadrele de conducere8, i.«mare acestea, pare o luptă fără sfârşit, iar criticile repetate pitind crearea unor noi clasificări confirmă motivaţia de a face»Mi lucru.

*Nevoia de a cunoaşte*. După cum s-a remarcat anterior, cu cât luh tunat ia este mai importantă (potrivit nivelului de clasificare), cu «Mi mai puţine persoane au acces la aceasta. În principiu, pentru a... hţinc acces la informaţii nu este suficient doar avizul de securitate. Ivi Mumele care doresc să obţină acces trebuie, de asemenea, să a»Miinusireze „o nevoie de a cunoaşte” aceste informaţii în vederea i1 h.h îi atribuţiilor oficiale. Acest aspect al sistemului de control”, mloi inaţiilor este mai puţin formal decât avizele de securitate; în prit ral, oricine gestionează informaţii clasificate este responsabil»! onlirmarea nevoii de a cunoaşte a unui solicitant înainte de a im m/a informaţiile respective9.

Nu se ştie cu siguranţă dacă această cerinţă reprezintă o barieră htientă împotriva transmiterii informaţiilor clasificate. În 1985, i Tunisia de Revizuire a Politicilor şi Practicilor de Securitate, de la I apartamentul Apărării (DoD), condusă de generalul în rezervă Richard M îl well, a constatat că „principiul potrivit căruia o persoană cu aviz, li securitate beneficiază de acces doar la informaţiile pe care «trebuie a le cunoas că, în general nu se aplică” 10.

I; u informaţii ar trebui clasificate?

«VI mai simplu răspuns la această întrebare, cel puţin în ceea ce I h iveşte Guvernul Statelor Unite, este oferit de definiţiile informaţiilor secrete, strict secrete şi strict secrete de importanţă deosebită de mai sus. În principiu, acestea pot părea simple, deşi termenii i Im „daune”, „daune grave” şi „daune deosebit de grave” sunt relui vagi, atât în sine, cât şi atunci când sunt aplicaţi unui concept *gomé* precum securitatea naţională.

De fapt, situaţia reală este chiar complicată. Modul în care a i”*«pusă problema – ce informaţii ar trebui protejate de accciul {j dezbaterea publice – presupune o viziune fundamental liberul! guvernului şi a societăţii, în care libera circulaţie a informaţiilor» regula, iar împiedicarea acesteia, prin mijloace de clasificare, excchl Probabil că această viziune constituie mai degrabă excepţia, fi HM regula. Până de curând, s-a aplicat doar confidenţialitatea guvif» namentală, eliminată doar atunci când guvernul considera că de/vi lui rea anumitor informaţii i-ar putea aduce un

beneficiu.

Gândiţi-vă, de exemplu, că statele democratice publică în intri curent un volum mare de date privind bugetele pentru apărare. I» «*v* într-o ţară democratică problema clasificării bugetului total peiiliti apărare iese din discuţie, guvernele nedemocratice obişnuiesc în facă lucrul acesta. De exemplu, Guvernul sovietic considera pânti * 1989 că sumele alocate bugetului pentru apărare sunt secrete dl stat; guvernele din China şi Coreea de Nord încă mai aplică aceantl regulă". Serviciile de informaţii din SUA alocă importante resurm pentru a stabili mărimea acestor bugete secrete pentru apărare; duci aceste informaţii nu ar fi considerate importante pentru Guvernul Statelor Unite, se presupune că resursele ar fi alocate pentru alle operaţiuni. Similar, dacă Statele Unite nu şi-ar publica bugetul pentru apărare, alte servicii de informaţii şi-ar redirecţiona resursele pentru n determina mărimea acestuia, iar statele adverse ar fi mai puţin sigure cu privire la capacităţile militare americane.

Prin acest exemplu dorim să susţinem *nu* că un stat democratic ai trebui să îşi clasifice bugetul pentru apărare, ci că motivul pentru care nu face acest lucru este legat mai mult de aspecte politice interne (obligaţia democratică potrivit căreia cetăţenii trebuie să ştie cu ce se ocupă guvernul pentru a-şi putea exercita drepturile şi îndatoririle politice) decât de criterii abstracte de clasificare. Problema poate fi pusă în felul următor: aproape orice organizaţie – partid politic, companie, echipă

de fotbal sau de alt tip – care se află în competiţie cu alte organizaţii doreşte să ţină secrete majoritatea informaţiilor cu privire la strategia sa de continuare a luptei, resursele ife Miitiilr şi aşa mai departe. În general, orice informaţie divulgată h«periclita poziţia competitivă.

A» «În lucru este valabil şi în cazul activităţilor unui guvern pitim! securitatea naţională. Problema este reprezentată *întotdeauna* în A%lrca unui echilibru între daunele care ar putea fi aduse la ţtă»*«securităţii naţionale şi imperativele unei ordini politice interne. În lui, nicio armonie între aceste două standarde şi nici nu pot fi jfcilmliaic clar.

hrsiunea pentru transparenţă nu vine întotdeauna din partea»M»lenilor. În ciuda tendinţei generale de păstrare a confidenţialităţii, mi îi *v* guvern – dar mai ales unul democratic – consideră adesea utilă «h i h iar necesară dezvăluirea unor informaţii pentru a-şi justifica puiule întreprinse şi a-şi atrage sprijinul cetăţenilor. După cum am tutu vai anterior, pentru a justifica şi a-şi asigura sprijinul public cu wlvlir la atacul cu bombă asupra Libiei din anul 1986, administraţia Huidui a dezvăluit informaţiile rezultate din decriptarea comuta,»itulor telegrafiate ale libienilor, potrivit cărora acest stat era Implicai în atacul terorist cu bombă de la o discotecă din Berlinul de U-i A Iertând Guvernul libian cu privire la interceptarea comunicaţiilor, «.liiunistraţia şi-a pus în pericol importante surse secrete.

*Supmelasificarea*. Au fost aduse critici

repetate la adresa Guvernului 4»un ican cu privire la clasificarea prea multor informaţii şi stabilirea unui nivel prea înalt de clasificare. Aceste critici au venit nu doar din iMiir. i comisiilor din Congres şi a analiştilor din serviciile secrete nu anumite administraţii, ci şi de la „cei din interior”. De exemplu, i omisia Departamentului Apărării din 1985 pe practici de securitate.i observat că:

par să fie clasificate prea multe informaţii şi că acestea au un grad de clasificare mult mai ridicat decât ar trebui. Politica actuală prevede că semnatarul unui document clasificat este responsabil de clasificarea atribuită, însă, de cele mai multe ori, din necunoaştere sau din grabă, nu se acordă atenţia necesară acestor proceduri. Similar, deşi sunt permise contestaţii la adresa clasificărilor neadecvate, sunt puţini cei care îşi fac îi mp să discute pe marginea acestor clasificări cu cel care le-a făcut12.

Într-o oarecare măsură, după cum am observat deja, confidenţi, ilitatea este o caracteristică normală a oricărui guvern. Dată fiind extraordinara deschidere a sistemului politic american, aceasta pl, al u»t pare anormală şi a ridicat mai multe obiecţii în Statele Unite det el ţ alte părţi. În ultimii ani, aceeaşi problemă a ieşit la iveală şi în t* state, în special în Marea Britanie, unde legile privind divulgarea InMmaţiilor guvernamentale sunt mult mai stricte decât în Statele UiilMP.

În afară de principala daună – obstrucţionarea inutilă a acer tulul cetăţenilor la informaţii, reducând astfel capacitatea acestora l»

înţelege şi de a face comentarii pe marginea politicii de secut Mato naţională –, supraclasificarea ar mai putea avea şi dezavantajat scăderii credibilităţii sistemului de clasificare, ceea ce ar putea ilu» la o tendinţă de ignorare a legilor, la nepăsare şi la „scurgeri «U informaţii” 14. Dacă vor fi clasificate multe documente inofenalvf, importanţa interdicţiilor privind divulgarea neautorizată a informaţilir clasificate se va diminua.

Este greu de spus dacă există o supraclasificare generali he Guvernul american. Deşi orice sistem care gestionează milioane dl documente în fiecare an poate produce rezultate nesigure, principali sursă de dezacord este reprezentată de existenţa unor puncte de vedere diferite referitoare la standardele care ar trebui aplicate atutwl când se hotărăşte gradul de clasificare. Părerea celor care susţin faptul că supraclasificarea este exagerată e că documentele suni deseori clasificate pentru a-i scuti pe oficialii guvernamentali di complicaţii sau de critici. Aceste persoane susţin, cu alte cuvinte, el de fapt clasificarea îi scuteşte pe oficiali de justificarea acţiunilot întreprinse. Deşi acesta este un motiv inacceptabil în ceea ce priveşti clasificarea, de cele mai multe ori situaţia este mai complicată; criticile sunt îndreptate adesea nu doar către un oficial care a greşit faţă de public, ci şi către guvernul însuşi în raport cu puterile străine15.

După cum s-a menţionat la analiza acţiunilor secrete, secretizaren se impune de cele mai multe ori din motive diplomatice, nu operaţionale Acest

lucru este valabil şi pentru activităţile de politică externă în general. Cu toate acestea, ca şi în cazul acţiunilor secrete, guvernele au avut tendinţa, în ultimii ani, să fie mai deschise cu privire la multe aspecte ale politicii externe şi să fie mai puţin preocupate de detaliile diplomatice. Există o probabilitate mai mare în prezent decât înainte ca guvernele să recunoască derularea unor acţiuni de spionaj şi a altor operaţiuni secrete. În acest fel, guvernul nu mai

(the Îi (niicat. Cu toate acestea, există posibilitatea ca motivele heNMiii *v*'s;1 fie întemeiate. De exemplu, în 1977, *The Washington mt* «§ iMfttţiuut că regele Hussein al Iordaniei ar fi primit unele ţfrt»HH din partea CIA, afirmaţie ce nu putea decât să-i creeze ţtitttM uncie dezavantaje în plan politic". Păstrarea secretului unei M! relaţii pentru a evita criticile şi periclitarea poziţiei politice i p fulul unui stat prieten reprezintă un motiv întemeiat pentru ÉMML/ale, deşi, din punct de vedere operaţional, acest lucru nu este Hiihiiu *kitbvtasificare*? Deşi se afirmă frecvent că guvernele au tendinţa bim«h a de a supraclasifica, merită studiat dacă în anumite domenii «lui amplă exact opusul. Acest lucru poate fi valabil în cazul iiftă Mintiilor generate în afara guvernului, care sunt suficient de in Linie pentru securitatea naţională, iar astfel se justifică clasi-H ui a şi controlarea lor. Cel mai concludent exemplu în acest sens»im minunăţiile legate de tehnologia armelor nucleare. Se presupune *»sie informaţii ce ar ajuta la proliferarea armelor nucleare ar fi iMuutf unui control riguros,

indiferent dacă provin din interiorul sau»lin uhu a guvernului.

Iu Statele Unite, această problemă a făcut obiectul Legii privind în igia atomică din 1954, care a definit datele secrete drept „toate»lim inaţiile privind (1) proiectarea, fabricarea sau utilizarea armelor mim Irai e; (2) producţia de materiale nucleare speciale; sau (3) utilizarea mini materiale nucleare speciale pentru producerea de energie” 17, i niilorm prevederilor legii, acest tip de informaţii sunt supuse. În îi i» talelor indiferent dacă datele provin din interiorul sau din afara guvernului. (Aceeaşi lege interzice şi diseminarea de informaţii «m laşificate privind proiectarea şi măsurile de securitate în cazul li veiselor centre de producere sau utilizare a materialelor nucleare) 18, i h toate acestea, în Statele Unite există foarte multe informaţii li, pic materiale şi arme nucleare la dispoziţia publicului – de aici şi linvestea conform căreia un strălucit absolvent de Fizică, lucrând cu în se deschise la o bibliotecă publică, a realizat planurile pentru e în unbă nucleară, pe care nişte experţi al căror nume nu a fost precizat I«au confirmat ca fiind viabile.

Printre alte informaţii care nu pot fi clasificate, dar care ar putea, în anumite situaţii, să beneficieze de protecţie se numără:

Informaţii financiare ce ar putea facilita câştiguri ilicite pe»l* (Mt de capital sau de mărfuri; informaţii tehnologice care nu trebuie dezvăluite inamicilnt informaţii personale ce ar putea permite unui serviciu à informaţii advers să recruteze oficiali guvernamentali fie i oferirea

unor sume de bani celor cu probleme financiare, fie *r* şantajarea lor.

Protejarea acestui gen de informaţii a implicat garantarea secui nu-l comunicaţiilor, despre care vom discuta în continuare. Câteihlttă însă poate implica şi alte aspecte. De exemplu, în Statele Unite i făcut eforturi în vederea aplicării reglementărilor privind exporta de tehnologie şi în cazul diseminării lucrărilor ştiinţifice legate 4 aceste tehnologii; cu toate acestea, nu a fost elaborată nicio strâng practică în vederea realizării acestui lucru. În 1982, directori adjunct al CIA, amiralul Bobby Ray Inman, a menţionat acea Mt problemă într-un discurs adresat American Association for în Advancement of Science. Vorbind despre cercetarea criptologii teoretică şi aplicată, el şi-a manifestat îngrijorarea faţă de faptul îl „publicarea la întâmplare a rezultatelor studiului respectiv va trefl interesul guvernelor şi entităţilor străine şi, prin aceasta, va produve daune ireversibile şi inutile intereselor de securitate naţională ni» Statelor Unite”. Dintre domeniile care ar putea aduce atingeif securităţii naţionale prin punerea în circulaţie a informaţiilor tehnic», Inman a amintit „echipamentele şi programele informatice, nil* tehnici şi mecanisme electronice, lasere, planurile agricole şi melo dele de fabricaţie” 19.

În anii de după 1982, extinderea criptografiei publice a dat naşten unei controverse majore în Statele Unite cu privire la controlul programelor informatice care conţin algoritmi complicaţi de criptare După cum s-a menţionat în capitolul 2, se

fac din ce în ce mai multe studii criptologice în sectorul privat, datorită utilizării tot mai largi a comunicaţiilor electronice în scopuri comerciale. Deşi acest lucru aduce beneficii importante din punctul de vedere al securităţii naţionale (de exemplu, comunicaţiile criptate pot contracara în cercările de furt tehnologic prin pătrunderea în serverele de e-mail sau în alte sisteme de comunicaţii ale unor companii), a generat îngrijorare cu privire la posibilitatea ca teroriştii, grupările de crimă

O«m»mm, de spălare de bani etc, să obţină acces la funcţiile de n-iiH, H«ceea ce va zădărnici eforturile de monitorizare a lor – n i-fiiiM de organele de aplicare a legii:

Im nu la avantajelor recunoscute ale criptării, am susţinut de mult timp i „h nu li – rărea criptării indestructibile – având în vedere capacitatea sa a».1 împiedica total organele de aplicare a legii din ţara noastră să ini» Inig.i fişiere pe care s-a pus sechestru şi comunicaţii interceptate l i iiiare la acţiuni ilegale, ce au fost criptate, iar apoi să poată acţiona miiipi pentru a combate activităţile periculoase criminale, teroriste şi a» «ptonaj şi a declanşa urmărirea penală – ar reprezenta o ameninţare «i masa şi radicală împotriva acestor interese centrale şi de o importanţă ijunurbită la adresa siguranţei publice20.

V a propus ca modalitate de reducere a acestui pericol controlarea Mpiiirului de software criptografic ce necesita algoritmi de criptare ilepaşeau o anumită „putere” (măsurată în funcţie de dificultatea cu it /olvare a cifrurilor rezultate)

21. În replică, producătorii ame-ii»m de software au susţinut că acest tip de controale asupra mjhuiului din SUA nu făceau decât să le permită competitorilor» lim’s;1 pună mâna pe o cotă de piaţă şi mai mare, în detrimentul nunelor americane22.

ttocuritatea

Măsurile de securitate sunt demersuri întreprinse în scopul blocării paie iiiţii unui serviciu de informaţii inamic de a culege date. Aceste mifimiri au ca obiectiv împiedicarea unui serviciu de informaţii advers Im să acceseze, fie să exploateze orice acces pe care îl poate avea la le i sonal, documente, comunicaţii sau operaţiuni în vederea obţinerii în h 11 date importante; ele reprezintă zidul care protejează minunăţiile clasificate. În această secţiune sunt analizate aspectele mai tradiţionale ale securităţii, care privesc protecţia împotriva h.i lurilor adversarului de a culege informaţii din surse umane; cele ne se referă la posibilităţile sale de culegere din surse tehnice sunt i na uzate mai târziu sub denumirea de „activităţi contrainformative imiliidisciplinare”.

Securitatea personalului

Securitatea personalului implică proceduri pentru verificarea HM didaţilor înainte de angajarea lor în posturi ce le oferă an în t» informaţii pe care un serviciu de informaţii advers le-ar pe.«considera interesante şi pentru garantarea faptului că actualii aiui.u – continuă să îndeplinească standardele necesare pentru a avea an în U astfel de date. Scopul principal al unei proceduri de verificare comit în evaluarea dorinţei

şi capacităţii potenţialului angajat de a ţiu secrete informaţiile clasificate. Elementele-cheie ale acestei evalul N sunt caracterul şi loialitatea potenţialului angajat23. Evaluam caracterului trebuie să ţină cont atât de stabilitatea mentali individului, cât şi de posibilitatea ca, dintr-un motiv sau altul, u««««să fie vulnerabil la şantaj din partea unui serviciu de informaţii advftt

*Investigaţiile*. În Statele Unite, procedurile de verificare stalul» dacă un individ poate primi aviz de securitate – adică acces autorim la informaţii clasificate. Investigaţia se bazează pe informatul, furnizate de către individ într-un chestionar de securitate, lui».* completată şi confirmată printr-o verificare la nivelul instituţiilor tit stat (consultarea bazei de date a diverselor organe de aplicare a legii a altor agenţii guvernamentale), şi, în funcţie de importanţa inlotmaţiilor la care va avea acces, se vor realiza interviuri cu prieteni cunoştinţe, foşti şi actuali vecini, colegi de serviciu şi de şcoală cu în cazul informaţiilor de o importanţă deosebită, se impune efectuarea unei reverificări periodice pentru menţinerea accesului. Dla mai multe motive însă, poate că aceste verificări de rutină *nu suni* foarte eficiente pentru a constata loialitatea şi caracterul personalului care va avea acces la informaţii clasificate.

Unele restricţii legale, care vor fi abordate în următorul capitol, împiedică FBI şi alte agenţii guvernamentale să obţină şi să păstrez* o listă a membrilor aşa-numitelor organizaţii subversive, chiar daefl ele militează în mod deschis pentru

înlăturarea violentă a guvernului Statelor Unite24. Un membru al unei astfel de organizaţii, care nu le-a spus cunoştinţelor sale despre apartenenţa sa la organizaţia respectivă şi nu a menţionat acest lucru pe formularele pentru avizul de securitate, are toate şansele să rămână nedescoperit.

Im plus, schimbările sociale din Statele Unite au făcut şi mai eşlli ila obţinerea unor răspunsuri sincere de la cunoştinţe, colegi, Hi lui şi alte persoane. În primul rând, există un resentiment tipic MHiitan faţă de verificările guvernului, ceea ce îi determină pe omlJ Hei nu fie dispuşi să transmită informaţii negative. Apoi, tfffipira mobilităţii geografice a societăţii americane îngreunează şi H”) umil localizarea fostelor cunoştinţe sau a foştilor vecini, care ihm mih pot avea doar informaţii superficiale în ceea ce-l priveşte pe l MMlldat. În anii ’90, cel puţin, climatul politic îi determina pe cei rkPilonaţi să nu ia foarte în serios întrebările despre loialitate şi

— Uvll Aţi subversive. Acelaşi lucru era valabil şi în ceea ce priveşte iMiiibarile despre caracter şi stilul de viaţă. De exemplu, creşterea

MiiMMuului de droguri în rândul clasei de mijloc (şi în special în i4 niliil tinerilor) în ultimele decenii face dificilă stabilirea cazurilor im care folosirea acestora în trecut indică o adevărată problemă de I«(tonalitate şi o potenţială vulnerabilitate în faţa şantajului.

Iu cele din urmă, se pune problema dacă există posibilitatea de «i i asigura pe informatori că informaţiile furnizate de ei vor rămâne MMihdenţiale. Potrivit Legii privind

confidenţialitatea din 1974, toanele au drepturi extinse de a accesa dosare guvernamentale cu Informaţii despre ele însele; deşi există o excepţie care permite unei iu-l iiuţii de anchetă să ascundă numele unui informator care solicită

1.1 mână sub protecţia anommatului, este posibil ca acest lucru să mm le ofere o siguranţă totală potenţialilor informatori, ce ar putea fi deranjaţi sau chiar mai rău dacă identităţile lor ar fi dezvăluite.

În primul rând, potenţialii informatori ar putea fi îngrijoraţi de posibilitatea ca numele sau datele lor de identificare (cum ar fi numere de telefon) să fie dezvăluite întâmplător. În al doilea rând, (h iar dacă identităţile lor nu sunt dezvăluite explicit, ei ar putea fi îngrijoraţi că persoanele care fac obiectul investigaţiilor vor putea să le deducă identitatea din totalitatea informaţiile existente în dosarele guvernamentale. (Cu alte cuvinte, transmiterea unui detaliu aparent nesemnificativ – pe care, oricum, numai informatorul îl ştia – ar putea să-i dezvăluie identitatea. Este posibil ca ofiţerul ce revizuieşte Jatele înainte de a le transmite să nu-şi dea seama că acest detaliu poate să conducă la identitatea informatorului şi ca urmare, să-l transmită, fără să conştientizeze răul provocat.) în fine, potrivit declaraţiilor făcute în 1978 de către un oficial de la Departamentul de Justiţie, la Comisia Juridică a Senatului, „teoretic, legile [privind confidenţialitatea şi libera circulaţie a informaţiei] sunt suficiente pentru a ne proteja sursele, dar este cu totul irelevant dacă chiar rei i «– să facă

lucrul acesta, atât timp cât sursele noastre cred contrariul” 1 O modalitate auxiliară de verificare a personalului este utilizam poligrafului, cunoscut şi sub numele de „detector de minciuni” Această tehnică a fost utilizată pentru prima dată de serviciile ilf informaţii din SUA; niciun alt serviciu de informaţii occidental sau neoccidental nu are aşa de multă încredere în acest aparat. În SUA, CIA a pus foarte mult accent pe utilizarea poligrafului. Agenţia a soliclUH ca orice candidat să fie supus unui test cu poligraful şi tot personalul i fie obligatoriu supus periodic acestui test. Cu toate acestea, utilizarea poligrafului în cadrul Guvernului american a fost combătută putemly de-a lungul anilor. Totuşi, în urma arestării pentru spionaj a lui Geoffrey Prime, angajat al Centrului Guvernamental Britanic pentru Comunicaţii (Government Communication Headquarters – GCHQ, agenţia britanică de interceptare a comunicaţiilor), oficialii americani i-au încurajat pe cei de la GCHQ să folosească şi ei metoda poli grafului. (Prime se pare că a compromis mai multe informaţii secrete provenind din surse tehnice, date ce indicau o strânsă cooperare între Marea Britanie şi Statele Unite.) Ameninţarea implicită a recomandării de a folosi detectorul de minciuni era că SUA ar fi mai reţinute în privinţa colaborării cu un serviciu secret care nu accepta o astfel de procedură. Deşi se pare că utilizarea poligrafului are un puternic efect de intimidare şi în multe cazuri duce la dezvăluirea unor informaţii ascunse, acurateţea sa rămâne încă sub semnul întrebării26. În afară de

frecvenţa cu care persoanele testate, deşi nevinovate, picau testul şi erau respinse sau forţate să demisioneze, serviciile de informaţii străine au elaborat metode de a „trişa” la acest test27. Cea mai evidentă dovadă în acest sens este cazul lui Aldrich Ames, ofiţerul CIA care a spionat aproape nouă ani pentru Uniunea Sovietică şi Rusia, din aprilie 1985 până în februarie 1994. De două ori în această perioadă (1986 şi 1991) el a fost supus testului cu poligraful28.

*Schimbarea tipului de ameninţare*. De la jumătatea anilor ’70, numeroase cazuri de spionaj au implicat angajaţi ai agenţiilor guvernamentale americane sau subcontractori29. Motivaţia principală în e... – a* imuri a fost cea financiară, sporită câteodată şi de o instaftll Mii emoţională30. Unul dintre cele mai complexe cazuri de acest ar mic cel al lui Robert Philip Haussen, agent FBI care a spionat! nun [imunea Sovietică şi Rusia cel puţin din 1985 până la arestarea li în 2 (M) I; mesajele sale către „manipulatorr sugerează o loialitate h» de serviciile secrete sovietice/ruseşti care nu are nimic de-a face mi Ideologia31.

Ai este cazuri diferă în mod clar de faimoasele cazuri de spionaj ihit i li a ne şi britanice din anii ’40 şi 50 (familia Rosenberg sau Kim Willhy), unde motivaţia era în principal ideologică. Acest exemplu «ugrica/a faptul că trebuie luate unele măsuri în vederea îmbuuHU (irii securităţii personalului, precum realizarea unor profiluri imiliologice detaliate sau crearea unui sistem de avertizare a cadrelor llinducere

atunci când o persoană cu acces la informaţii clasificate h» ne află într-o situaţie financiară dificilă, fie pare să aibă un stil de viem dincolo de posibilităţile sale financiare.

nncuritatea fizică n uiitatea fizică se referă la metodele utilizate pentru a împiedica în «esiil fizic al agenţilor străini la informaţii clasificate. Se referă ia iniţatea locurilor în care sunt stocate informaţiile clasificate şi la i uiacteristicile sistemelor de alarmă pentru detectarea pătrunderilor... unorizate în zonele cu acces restricţionat şi, mai mult, sisteme sofis-ili ale cu parole pentru protecţia informaţiilor clasificate stocate în calulaioare32. În mare parte, condiţiile de asigurare a securităţii fizice suntunoscute şi diferă foarte puţin sau deloc de măsurile pe care orice i «impartie le întreprinde pentru a împiedica furturile de produse, echipamente sau informaţii şi documente interne de importanţă deosebită.

Ü diferenţă majoră este, totuşi, că securitatea fizică are ca scop nu doar protejarea obiectelor materiale, cum ar fi documentele, care «ouţtn informaţii, ci şi a informaţiilor în sine. Acest lucru presupune – untroale mai severe ale accesului în zonele respective şi la echipamentele folosite acolo, având în vedere că un intrus ar putea planta inarte uşor un dispozitiv de interceptare, iar serviciile de informaţii ui verse ar avea astfel acces la zona restricţionată33. De aceea, este important ca tot ceea ce intră şi iese din acea zonă să fie supus, ontrolului.

La fel, este foarte importantă existenţa unor dispozitive de minare a zonei pentru a detecta

orice dispozitiv de interceptate Acest lucru atrage după sine dezvoltarea unor sisteme de interceptez a conversaţiilor, mai greu de detectat. Cel mai înalt nivel ** tehnologie la care s-a ajuns în cadrul acestei spirale a perfectlonifu sistemelor de detectare a ajuns în atenţia publicului într-un»h»u incidente în care a fost implicată Ambasada Statelor Unitö»Im Moscova. În anii ’70, de exemplu, o antenă sovietică a fost descopeilÜ în şemineul Cancelariei (clădirea ambasadei). Apoi, în anii ’80,» «descoperit că un număr semnificativ de maşini de scris electrice avenu dispozitive de interceptare34. Mai târziu, a ieşit la iveală faptul e sovieticii compromiseră virtual întreaga structură a noii Cancelarii pe care SUA o construiseră acolo. Sovieticilor li s-a permii ** realizeze, fără a fi supravegheaţi de către americani, coloanele grinzile din beton prefabricat din care a fost construită Cancelaria Sovieticii au profitat de această eroare de securitate şi au proiectat utt sistem de interceptare care utiliza întreaga structură ca antenă pentru interceptarea semnalelor şi transmiterea acestora. Sistemul era foarte sofisticat, iar Statele Unite nu au înţeles nici până acum cum funcţiona”.

Contraspionajul

Măsurile de securitate despre care am discutat sunt pasive, adică nu încearcă să contracareze acţiunile serviciului de informaţii advers, el urmăresc doar să împiedice accesului acestuia la informaţii. Măsurile mai active, ce urmăresc înţelegerea modului în care acţionează un serviciu secret concurent în vederea

contracarării şi combaterii acţiunilor lui şi a culegerii de informaţii în scopuri proprii, sunt cunoscute sub numele *contraspionaj*.

Operaţiunile de supraveghere

O modalitate clară de a afla despre activităţile unui serviciu de informaţii advers este iniţierea unor acţiuni de supraveghere a ofiţerilor acestuia (monitorizarea permanentă) oriunde aceştia operează. O astfel de supraveghere încearcă să stabilească unde se deplasează ofiţerii şi îl» îmi omunică sau cu cine intră în contact; aceste contacte pot fi – l. ulterior pentru derularea unei anchete!»., i conceptul e simplu, în practică este vorba despre o activitate fMMplmiv Abilităţile speciale ale ofiţerului, despre care am discutat imuini din perspectiva culegerii de informaţii din surse umane, h-m.i. să servească înainte de toate contracarării acest tip de acti-mmu I) liţerul va fi instruit să evite propria monitorizare şi va folosi thutr Ile „predare-fulger” şi căsuţa poştală impersonală pentru a Ifemulr identitatea persoanelor cu care ia legătura. În plus, dacă va I ilajul, ofiţerul poate anula orice întâlnire planificată pentru lvita punerea în pericol a sursei sale. Este deci important ca tţ»iii (iunile de supraveghere să fie mascate. Acest lucru este însă. Imiul de greu de realizat şi presupune un număr mare de persoane, lud tu vedere că ofiţerul instruit în tehnici de contrafilaj va observa 4 ai traşi persoană îl urmăreşte de o perioadă de timp.

I und o tehnică atât de complexă şi de costisitoare, este important.u casta să fie folosită efectiv în cazul unor ofiţeri de informaţii, iwipile

care trebuie supravegheate, având în vedere că reprezintă hau tu oficiale în care ofiţerii serviciilor de informaţii activează în un lor sub acoperire, sunt: diplomaţi, ofiţeri consulari, reprezentanţi

...(reiau, jurnalişti care lucrează pentru presa acreditată de guvern îi ungajaţi ai organizaţiilor internaţionale, precum ONU, atunci când «vila sunt selectaţi de către guvernele ţărilor respective. Problema ar identificarea celor care ocupă astfel de poziţii şi care sunt cu adevărat ofiţeri de informaţii.

Sunt mai multe moduri de a rezolva această problemă. În general, Lu, 1 un ofiţer deţine informaţii exacte despre modul de funcţionare îi unei anumite ambasade străine, de exemplu, atunci poate spune un dintre oficiali îşi desfăşoară cu adevărat activitatea diplomatici»au consulară. Dacă unul dintre oficiali nu pare interesat de acti-s naica sa, atunci el poate fi implicat în culegerea de informaţii.

Mai este posibil, de asemenea, ca, observând tehnicile de rotaţie, i de înlocuire a personalului, să se poată stabili cine înlocuieşte pe ine; dacă X a fost identificat ca fiind ofiţer de informaţii, atunci postul său va fi preluat, cel mai probabil, tot de un ofiţer de informaţii. Aceleaşi tehnici folosite în general pentru culegerea de informaţii pot fi îndreptate şi către un serviciu de informaţii advers a către agentul unui astfel de serviciu care acţionează pe teritoriul altui stat. Cu cât se ştiu mai multe informaţii despre servi»*»! respectiv şi despre modul de funcţionare a acestuia, cu atât mal UN) va fi realizată operaţiunea de filaj. În cele

din urmă, agenţii diihil, despre care vom discuta mai târziu în cadrul acestui capitol, *4 stabili identitatea ofiţerilor de informaţii străini.

Culegerea informaţiilor

Cea mai bună modalitate de realizare a obiectivelor contraspionajului este culegerea informaţiilor direct de la serviciul advers, prin mijloat* umane sau tehnice. De exemplu, imediat după cel de-al Doliu Război Mondial, agentul sovietic Kim Philby, care lucra în cadrul MI6 (Serviciul britanic de informaţii externe) le-a furnizat agen (llcM KGB informaţii prompte privind unele operaţiuni secrete din statali baltice, Ucraina, Rusia şi Albania. Până în 1951, când Philby a fiul forţat să demisioneze din MI6, acesta deconspirase, potrivit utilmaţiilor sale, sute de agenţi britanici şi americani. În mod asemănător, serviciul de informaţii britanic beneficia, la începutul anilor ’70, dl sprijinul adjunctului şefului de misiune din Londra, Oleg Gordievskl Gordievski i-a asigurat pe britanici că KGB nu avea niciun agent infiltrat în MI5 sau MI6 şi în 1983 i-a avertizat imediat asuprit faptului că un ofiţer MI5 care fusese dat afară se oferise să spionc/e pentru KGB36.

Potrivit acestor exemple, activitatea de contrainformaţii nu este foarte diferită de cea de culegere a informaţiilor în general, însă are ca ţintă serviciul de informaţii advers, şi nu guvernul, forţele armate sau alte instituţii.

Defectorii şi agenţii dubli

Ca şi în cazul celorlalte tipuri de culegere a informaţiilor *humint* îndreptate către o societate

închisă cum era fosta Uniune Sovietică, recrutarea şi dirijarea unui agent în interiorul unui serviciu de informaţii este o sarcină extrem de dificilă. Astfel, în trecut, Statele Unite şi alte state occidentale se bazau foarte mult pe defectori ai serviciilor de informaţii sovietice pentru contraspionaj. Vitali Iurcenko, directorul adjunct al departamentului de spionaj împotriva Stateloi Unite şi Canada din cadrul KGB, este un exemplu în acest sens t-l»fi i e a defectat în vara anului 1985, a furnizat informaţii despre Eretele spionajului sovietic împotriva Statelor Unite. De exemplu, fH iunie că nu le cunoştea numele reale, în urma detaliilor personale tMjKHaţionale pe care acestea le-a furnizat, Ronald Pelton, un fost, al Agenţiei Naţionale de Securitate, a fost arestat, iar Edward lhoward, un fost angajat al CIA, a fost pus sub acuzaţie37.11 aiul metodă importantă de realizare a contraspionajului este

…intermediul agenţilor dubli. Ei sunt agenţii ce, deşi pretind că lunca/a pentru un serviciu advers, de fapt sunt controlaţi de către Utilul pe care se presupune că îl spionează. Este posibil ca ei să fii Mi la origine spioni şi, ca urmare a deconspirării lor, să fie con – Miip în agenţi ai ţării în care au fost prinşi. Sau mai pot fi „falşi»Mm lori”, agenţi care se oferă să spioneze pentru un serviciu de uilonnaţii inamic, dar care de fapt rămân loiali ţării lor. Între cele tlMtia categorii ar mai fi persoanele care, fiind abordate de către un nu viciu de informaţii inamic, au raportat încercarea de recrutare suini ilarilor şi au fost încurajaţi să intre în joc.

Aceste operaţiuni care implică agenţi dubli servesc aceloraşi îi opuri contrainformative. La cel mai simplu nivel, ele permit unui". viciu de informaţii să înţeleagă metodele secrete ale adversarului ti.a identifice ofiţerii din serviciul de informaţii advers care sunt implicaţi în recrutarea de agenţi. Ca urmare, operaţiunea de supra-h pliere poate viza adevăraţii ofiţeri de informaţii, acordându-le mai pu pus atenţie celorlalţi oficiali care sunt într-adevăr diplomaţi, ataşaţi oiuerciàli etc.

IV lângă identificarea ofiţerilor de informaţii din serviciile adverse „u «sie operaţiuni îi ajută pe ofiţerii de contrainformaţii să afle «iiriodele operative utilizate de adversarii lor. Folosind agenţi dubli, pup afla cum procedează manipulatorii pentru a transmite instrucţii către sursă şi a primi informaţii de la aceasta, când şi unde pu Icră să se întâlnească, ce precauţii îşi iau pentru a nu fi descoperiţi „i ni.d. Pe scurt, cunoscând modalitatea şi locul în care adversarul îi legătura cu sursele sale, ofiţerii de contrainformaţii află despre iliililăţile adversarului şi se poate proteja mai bine de acesta. Mai umil, cunoaşterea abilităţilor adversarului şi a tipului de activitate al»îi (erilor de informaţii contribuie la identificarea acestora de către.m viciul contrainformativ. În cele din urmă, dacă un agent dublu «ic dotat cu echipament special, cum ar fi un transmiţător radio, creat special pentru a fi utilizat de către agenţi, atunci serviciul îl informaţii respectiv are şansa de a-l studia. Acest lucru ar puteţi tiu* la interceptarea comunicaţiilor

radio dintre ofiţerii de informul!! «serviciului inamic şi adevăratele lor surse.

Din instrucţiile pe care le primesc agenţii de la manipulwhiH, un serviciu de informaţii poate afla care sunt datele prioritare pei HMI serviciul de informaţii advers. De asemenea, acest lucru mai înmMJ oferi indicii valoroase cu privire la strategiile altor servicii de informaţii.

Una dintre cele mai interesante controverse din istoria serviellltit de informaţii are în prim-plan instrucţiile privind culegere» dl informaţii furnizate unui agent dublu britanic (nume de cod „Tricicleta”) de către serviciul de informaţii german cu puţin timp înainte dl intrarea Statelor Unite în cel de-al Doilea Război Mondial. Agentul, trimis în Statele Unite pe la jumătatea anului 1941, a avut la el în chestionar în care, printre altele, cerea informaţii detaliate cu priviri la bazele americane din Hawaii. Informaţiile oferite FBI de călt» agentul dublu, respectiv lista întrebărilor şi posibila semnificaţie, ut! fost ignorate total de aceştia38. Oare, dacă serviciul de informtilll american ar fi exploatat mai bine această informaţie, ar fi putut! anticipa atacul trupelor japoneze de la Pearl Harbor?

De asemenea, lipsa de interes faţă de un domeniu destul»I«important ar putea indica faptul că serviciul advers deţine de* informaţii în acest sens; acest lucru ar putea reprezenta un indiciu important pentru activitatea de contrainformaţii.

În afară de obţinerea unor informaţii despre serviciul advers, modul de funcţionare al acestuia şi priorităţile privind culegerea informaţiilor,

agenţii dubli pot exercita un anumit control asupra acţiunilor întreprinse de serviciu. Simpla existenţă a unui agent dublu este suficientă pânfl la un anumit punct; dacă serviciul advers ştie că are un agent cu acces la informaţii specifice, nu se mai deranjează să recruteze un altul. Dacă agentul dublu reuşeşte să contracareze activităţile serviciului, atunci acesta poate proteja informaţii importante. În orice caz, dirijarea agentului dublu presupune mult timp şi efort din partea ofiţerului din serviciul de informaţii advers, reducând astfel resursele disponibile pentru recrutarea şi coordonarea adevăraţilor agenţi.

Mai mult, beneficiul pe care un agent dublu îl reprezintă în cadrul operaţiunilor serviciului advers poate conduce la recrutarea r*»tuies a altui agent dublu, care poate avea acces la informaţiile jÉftritr serviciului advers. Primul agent dublu poate garanta pentru li fiii al doilea; de exemplu, primul agent ar putea confirma, sălmm faptul că al doilea tocmai a fost avansat într-o funcţie care îi hhilh.i un larg acces la informaţii deosebite sau că are probleme ftthhi inie şi are nevoie disperată de o altă sursă de venit.

Ivuliu a rămâne credibili, agenţii dubli trebuie să fie capabili să îl mult e informaţii manipulatorilor lor. De cele mai multe ori, această f-ttli Cm;1 se rezolvă cu aşa-numitele informaţii „de umplutură” – … în informaţii clasificate, de o importanţă deosebită, care de fapt im itiitl aşa de importante. Alternativ, agentul dublu mai poate furniza şi informaţii reale şi importante pe care

serviciul inamicul le-a atipiiul deja pe alte căi. În astfel de cazuri, serviciul de informaţii 14 m dirijează agentul trebuie să se gândească bine dacă va menţine hm Uluiitatea acestuia şi să contribuie la dublarea informaţiei iMiiiuse de agent, întărindu-i astfel credibilitatea. Scopul este de a i.1 u ai mai puţine informaţii utile fără a trezi suspiciunea serviciului». minunaţii advers.

I) altă modalitate mai ambiţioasă de a-i folosi pe agenţii dubli a i pune să furnizeze tot felul de informaţii şi dezinformări cu i.«pul de a induce în eroare serviciul advers. Până la un anumit puni i. această modalitate controlează nu doar informaţiile culese de inamic, ci şi capacităţile analitice ale acestuia. Rezultatele pot fi. «iiaordinare, deşi dificultăţile întâmpinate pot fi pe măsură39.

Dezinformarea este discutată pe larg în capitolele următoare. Veastă secţiune analizează două exemple de operaţiuni majore l» se însurate de agenţi dubli, foarte reuşite, una pe timp de război şi, daltă pe timp de pace.

*Agenţi dubli din timpul războiului*: *sistemul încrucişat*. Una dintre cele mai cunoscute operaţiuni majore desfăşurate de agenţi dubli este Sistemul încrucişat, prin care britanicii, aproape pe întreaga perioadă a celui de-al Doilea Război Mondial, „au dirijat şi în controlat spionajul german din ţara lor” 40. După ce au prins un lient german la întoarcerea acestuia din Germania în Marea Britanie. h iar la începutul războiului”, britanicii au construit o reţea de presupuşi agenţi germani, lăsându-i pe germani să creadă în ei

până la sfârşitul războiului.

Printre altele, agentul iniţial a furnizat informaţii în baza i Al germanii au emis acte de identitate false pentru a trimite alţi ayi care urmau să fie paraşutaţi sau transportaţi cu barca, lin Hi têtu astfel capturarea lor de către britanici. În alte cazuri, noii»ujh* trebuiau să-i contacteze pe cei care erau deja în activitate (contint de către britanici) pentru bani sau alt fel de ajutor. Până la st Ai ÎI războiului, beneficiind de o anumită şansă, britanicii au reull 4 controleze întreaga reţea de spioni germani, interceptându-i pe t-l noi la venirea acestora.

John Masterman, ofiţerul MI5 care a coordonat acţiunea, l «fixat şapte obiective:

controlarea reţelei de spioni a inamicului; capturarea noilor spioni infiltraţi în ţară; identificarea persoanelor şi a metodelor folosite de către servieta! de informaţii german; obţinerea unor informaţii despre codurile şi cifrurile serviciului german; obţinerea unor informaţii despre planurile şi intenţiile inamicului prin chestionarea agenţilor acestuia; influenţarea planurilor inamicului prin răspunsurile trimlii acestuia; dezinformarea inamicului cu privire la planurile şi intenţiile Marii Britanii.

Avantajele britanicilor au fost enorme. De exemplu, în 1940, agentul iniţial a primit de la Berlin un cod pentru a putea să comunici cu Germania. Deoarece acest cod s-a dovedit a sta „la baza mal multor coduri folosite de Abwehr [serviciul de informaţii militat german]”, faptul că britanicii au intrat în posesia lui „i-a ajutat %*K*

cunoască în întregime şi de timpuriu sistemul [codului Abwehr]" Atunci când războiul a avansat, iar britanicii au devenit mai siguri pe Sistemul încrucişat, ei şi-au îndeplinit şi ultimele două obiective menite să îi inducă în eroare pe nemţi. Punctul culminant a fost în 1944, când agenţii dubli au fost folosiţi pentru a susţine stratagema prin care nemţii au fost convinşi că debarcarea din Ziua Z va avea loc la Calais, şi nu în Normandia42.

Datorită acestui succes al criptologiei (Ultra), serviciile de informaţii britanice au putut studia reacţia germanilor la informările şi înfittfiii marile raportate de agenţii dubli. Printre altele, au pulul ttotivii rare dintre rapoarte erau înaintate înaltei conducere din Imlim»I dacă liderii aveau încredere în informaţiile furnizate. Acest toiiti.h k a fost vital pentru atingerea obiectivului de dezinformare. ÉtMinc le-a permis britanicilor să scoată în evidenţă anumite pihfhifr pe care nemţii le trecuseră cu vederea sau să modifice IHMH«În pentru a alunga orice umbră de îndoială din partea germanilor. Controlarea reţelei de spionaj inamice a avut însă preţul ei:

„U trebuia să producă suficiente informaţii încât să satisfacă Muliihe germanilor. În plus, informaţiile pe care le producea nu imehiii h combătute prea uşor cu ajutorul informaţiilor primite de thinani pe alte canale de culegere a informaţiilor, inclusiv de la iMtn iipali spioni ce nu fuseseră capturaţi. (S-a dovedit că aceştia nu MUlau, dar, desigur, britanicii nu puteau să îşi dea seama de acest Im în decât în timp; la început au fost nevoiţi să presupună că ar „a" h exista alţi

agenţi despre care nu ştiau.) Cu toate acestea, preţul uit nu părea prea mare; din moment ce era posibil ca germanii să 4 ihn o reţea de spionaj în Marea Britanie, era normal ca britanicii să a lluiducă.

«coordonatorul Sistemului încrucişat considera mai târziu că poate»I) i colegii săi au fost prea precauţi, în sensul că britanicii au fui m/al probabil mai multe informaţii reale decât era nevoie şi nu au ini»sii la maximum resursele de care beneficiau pentru a induce în i mare inamicul. Nu numai că germanii aveau mult mai puţine canale umliare de informaţii decât credeau britanicii, prin care să verifice inioi mâţule din Sistemul încrucişat (aşa cum am menţionat mai sus, unu aveau niciun agent loial), ci au dovedit a avea extrem de multă îi h icdere în agenţii pe care îi considerau a fi în serviciul lor. Acest în ad ridicat de încredere este ilustrat şi prin eşuarea următorului plan:

I, a un moment dat, unul dintre agenţi a fost dirijat ţi s-a ordonat să se comporte într-un anume fel] pentru a le arăta germanilor că este sub control, obiectivul fiind ca aceştia să îşi facă o idee falsă asupra metodelor noastre de a manipula un asemenea agent şi el să îi convingă astfel că şi ceilalţi agenţi sunt loiali. Teoria s-a dovedit a fi una înţeleaptă, iar gafele comise au fost imense şi flagrante, însă obiectivul nu a fost atins… Germanii credeau în continuare despre agent că este onest şi loial!

*Agenţi dubli pe timp de pace*: *operaţiuni ale Cubei înipon*r *Statelor Unite*. Pe 12 august 1987,

*The Washington Post* relata» «în dezertor din serviciul cubanez de informaţii externe (DGI) Io el 1 declarat investigatorilor CIA că „un număr nedeterminat de ottt IÉ din Guvernul cubanez, pe care Statele Unite îi bănuiau de colahuinn secretă cu CIA, ofereau agenţiei informaţii false sau i releva»** pregătite de DGI Cuba" 43. În urma acestei dezvăluiri, presa cuhaia «a publicat relatări detaliate ale operaţiunilor acestor agenţi duNH» incluzând fotografii ale lor în timp ce desfăşurau presupuse activiim» clandestine. Faptul că activităţile lor erau cunoscute de cubain până în cele mai mici detalii pare să confirme ipoteza că au (– agenţi dubli cel puţin o parte din dacă nu chiar pe toată perioada N care se presupune că spionau în Cuba. Conform unor surse cubaneu, unii dintre agenţi, conştienţi de faptul că americanii cunoşteau adevărata lor apartenenţă, le-au trimis mesaje de rămas-bun cooi donatorilor lor din Statele Unite.

Fără a face o analiză atentă a informaţiilor furnizate de acoH agenţi dubli, nu se poate stabili dacă în Cuba se desfăşura o campanii menită să inducă sistematic în eroare Statele Unite pentru a acţiona contrar intereselor proprii. Chiar şi în absenţa unui asemenea plaa ambiţios, operaţiunea ar fi meritat din punctul de vedere al Cubei, deoarece ar fi necesitat efort şi timp din partea CIA, distrăgfind astfel atenţia agenţiei de la informaţiile utile; de asemenea, ar fi ieşit la iveală metodele operaţionale ale CIA, neutralizând astfel agenţii reali, dacă ar fi existat; şi, nu în ultimul rând, sistemul Statelor Unite de analiză a

informaţiilor secrete ar fi fost asaltat de date reale sau false menite să creeze confuzie şi să împiedice SUA că îşi formeze o imagine de ansamblu asupra evenimentelor din Cuba”.

Activităţi contrainformative multidisciplinare (MDCI)

Ce este MDCI?

Ameninţarea în materie de culegere a informaţiilor reprezentat A de un adversar ce deţine tehnologie de ultimă oră nu se limitează la culegerea datelor din surse umane. În acelaşi fel, acţiunile fPMliih h inative active nu se pot limita la contraspionaj. Din contră, S iiti Mii luat în considerare întregul arsenal cu care adversarul ar fi*» ««alege informaţii din surse tehnice, cum ar fi fotografierea fUM MihK a şi interceptarea comunicaţiilor sau a transmiterii de

Aulei, principala sarcină a MDCI este de a evalua eficienţa e«în t li îi adversarului pentru culegerea informaţiilor din surse pus* *v* (unoaşterea acestor aspecte indică punctele vulnerabile ale pramatiilor, comunicaţiilor sau activităţilor şi ajută la găsirea celor mi hune modalităţi de protejare a acestora. Măsurile ce pot fi luate ştirii li etichetate ca „măsuri tehnice” sau „de securitate şi variază p fum ţie de tehnologie. Cu toate acestea, perspectiva multidis-I ifiliuai, 1 este importantă deoarece ne încurajează să privim problema 4»i«punctul de vedere al adversarului – adică să luăm în considerare imn jiul spectru de resurse de care acesta dispune.

miu uritatea comunicaţiilor

Am i iun interceptarea mesajelor, atât a celor

scrise, cât şi a celor în Uniuni electronic, este una dintre cele mai importante metode de mie pere a datelor, protejarea conţinutului lor este de multă vreme o nu mă a serviciului de contrainformaţii. Încă de la începutul secolului XX, s-a pus accentul pe protejarea comunicaţiilor electronice în uisinise prin cablu sau unde radio.

Mesajele transmise prin cablu pot fi protejate fie prin prevenirea i.iieu eptării liniilor de transmisie a comunicaţiilor (citirea mesajului), fie prin extragerea unei mici cantităţi de curent de pe linie sau im în interceptarea fluctuaţiilor câmpului magnetic din jurul liniei... m/al de curentul ce trece prin acesta. Cablul din fibră optică este în sigur, deoarece interceptarea mesajelor transmise pe această de s-a dovedit a fi o problemă45. Semnalele radio, în schimb, nu i»în li protejate în general; orice receptor de pe raza respectivă le l»i»ale intercepta. Unele semnale, cum ar fi transmisiunile privi în rounde (folosite, printre altele, pentru apelurile telefonice la hsianţă), sunt unidirecţionale (nu se dispersează în toate direcţiile, i sunt concentrate într-un fascicul rază îndreptat spre destinatar), în chiar şi acestea pot fi interceptate dacă receptorul este în aria de îi superire a emiţătorului.

Conţinutul mesajelor radio era protejat la început prinul Mtă Mesajele scrise pot fi criptate în mod tradiţional înainte de ţ transmise. În trecut, când se utiliza semnalul analog pentru *hm* miterea mesajelor vocale, se foloseau „telefoane sigure” „dispozitive de bruiaj”; acestea distorsionau semnalele voce IMN manieră

complexă. Oricine intercepta un astfel de semnal auze* în amestec de sunete fără sens, asemănătoare combinaţiei de IHUI dintr-un text cifrat. În principiu, reconstituirea textului originel «» la fel de dificilă. În prezent, atunci când mesajele voce sunt traittlnti în formă digitală, se aplică metode de criptare mai sofisticate

Telefoanele sigure sunt relativ scumpe şi sunt folosite în prim l» pentru a transmite informaţii clasificate. Nu sunt des utilizate, el folosesc mai ales de către executiv. Astfel, majoritatea comunicatlliw telefonice la distanţă, care folosesc transmisia prin microunde, *h* printr-o reţea de turnuri (microunde terestre), fie între staţii tereM* şi sateliţi, sunt vulnerabile la interceptare.

La mijlocul anilor ’80 în Statele Unite, această situaţie a capü atenţia publicului din cauza controversei privind locaţia noii Ambanaè sovietice de la Washington. Construită în cartierul Mount Aldo, d înălţime faţă de centrul oraşului, ambasada şi clădirile anexe em poziţionate deasupra centrului oraşului Washington şi a Virginiel É Nord, inclusiv deasupra Casei Albe, a Departamentului de Stat, i Pentagonului şi al majorităţii clădirilor guvernamentale. Din ace Me clădiri se pot intercepta numeroase apeluri telefonice la distanţă, mi şi din alte clădiri oficiale ale Rusiei din Statele Unite (consulate reprezentanţe comerciale din New York, Washington şi San Francisco misiunea ONU din New York; facilităţile rezidenţiale şi de recreete din New York City, Long Island şi de pe coasta estică din Maryland)

Pe lângă faptul că oficialii guvernamentali folosesc telefoane nesigure, posibile ţinte ale culegerii de informaţii prin astfel de mijloace pot fi şi diverse companii de tehnologii avansate, comercianll de bunuri ce furnizează anumite produse pe care un stat le vinde sau le cumpără în cantităţi mari (cereale, petrol şi aur), precum l instituţii financiare. Un serviciu de informaţii ar putea, de asemenea, să vizeze indivizi ce au acces la informaţii clasificate pentru a afla detalii compromiţătoare din viaţa lor personală, cu scopul de a-i şantaja

Au fost sugerate numeroase măsuri de prevenire pentru a reduce această vulnerabilitate. Spre exemplu, se poate revizui reţeaua ele fHM" hhele pentru a elimina astfel riscul ca traseul să treacă pe lângă me» în interceptare cunoscute sau potenţiale, folosindu-se cabluri iÜtMiir la alternativă, se poate cripta semnalul transmis prin «mhimlc prin bruierea lui atunci când se emite pentru prima dată *se** * ipiaiea lui după ce a parcurs porţiunea respectivă de microunde. W* În soluţii au hibe tehnice, iar implementarea lor presupune tutun i destul de mari. Situaţia ar putea fi rezolvată prin folosirea iiptice, soluţie adoptată de companiile de comunicaţii din unit* economice. Cablurile de fibră optică nu sunt mai puţin».ialule la interceptare, dar, datorită capacităţii mari (se pot iMttiuuic simultan mai multe semnale), au costuri mai mici decât uMuiile de cupru tradiţionale sau reţelele terestre.

*hm* imtatea emisiilor

Mm echipament electric emite unde

electromagnetice; teoretic,»în interceptarea acestor unde este posibilă determinarea caracitalicilor semnalelor electrice în urma cărora au fost emise. Astfel, j» în pl, elucrarea acestor „unde” numite „emisii”, se poate reconstitui im lui unui document tipărit pe o maşină de scris electrică sau iMimuns de la un computer către imprimantă. Se pot lua măsuri de un ui iiate în acest sens prin protejarea echipamentului electric pentru t. ilut crea intensităţii emisiilor, făcând dificilă interceptarea acestora.

Alin măsuri tehnice de securitate în pot lua anumite măsuri de protecţie împotriva altor forme de niedere a informaţiilor prin mijloace tehnice. În ceea ce priveşte iipiuvegherea şi fotografierea prin satelit, este posibil să se anticipeze lulele acestora şi să s-o avertizeze obiectivele militare sau alte luective de importanţă pentru ca acestea să înceteze activitatea şi să una la adăpost echipamentele de importanţă deosebită, în locuri iulie satelitul nu le poate fotografia; acest lucru este posibil în «indiţiile în care s-ar putea stabili cu exactitate care dintre sateliţii iiiversarului sunt folosiţi pentru recunoaştere fotografică. Desigur, îi cât se ştie mai mult despre capacităţile sateliţilor, cu atât este mai isor să se ia măsurile de prevenire necesare. Spre exemplu, după ce se determină punctele de pe suprafaţa terestră aflate exact lui) *wkm* satelitului, este necesar să se cunoască la ce distanţă, în Ui parte, obiectele sunt încă în raza camerei. Similar, culegerea ein loc* a informaţiilor sau prin telemetrie, poate fi prevenită prin ui Nt* bruiaj, schimbarea frecvenţei

sau încetarea emisiei atunci eţ adversarul este în apropiere.

Dezinformare şi contradezinformare

Până acum, prin discuţia despre contrainformaţii, am încerc»! 4 studiem diversele modalităţi prin care poate fi prevenită culcau, datelor de către adversar. În caz de succes, adversarului îi vor fi probabil informaţiile necesare pentru a analiza situaţia în care află, iar acţiunile sale, în orb, nu vor servi intereselor uriu Atlle După cum a rezultat din discuţia despre operaţiunile agenţilor dultll în încercarea de a contracara operaţiunile adversarilor de culegere informaţiilor este mai eficientă concentrarea asupra capacităţii.* acestuia de a analiza informaţiile secrete – şi anume încercarea de I dezinforma.

Ce este dezinformarea?

Dezinformarea reprezintă încercarea de a conduce pe o pistă gref IU analiza informaţiilor efectuată de adversar în ceea ce priveşte situaţii politică, militară sau economică. În consecinţă, formându-şi o imagine greşită asupra situaţiei, adversarul va acţiona în dezavantajul său Aceasta este considerată o formă de acţiune contrainformativă deoarece urmăreşte să facă inutile operaţiunile de culegere a informatului desfăşurate de adversar; în plus, de cele mai multe ori sunt implicate metode contrainformative, cum ar fi operaţiunile agenţilor dubli.

Dezinformarea este un concept asemănător cu eşecul unei acţiuni de culegere a datelor. O

acţiune de dezinformare reuşită înseamnă eşecul operaţiunii de culegere a datelor desfăşurate de adversar Există şi reversul, desigur; una dintre părţi poate face greşeli importante în analiza datelor chiar şi fără dezinformarea din partea adversă. Cu toate acestea, în cazul nereuşitei acţiunii de culegere a

§e»în m* poate identifica efortul părţii adverse de a dezinforma. În 9 inunuia acest efort este responsabil pentru eşec e o chestiune mai ht1" «UI.

În» poate recurge la dezinformare atât pe timp de pace, cât şi pe mnp tir război, deşi, din diverse motive, este de aşteptat ca dezin-Itfii Mica să fie mai des utilizată pe timp de război.46 Dezinformarea jMir li lactică sau strategică. Exemplele de dezinformare strategică tu-a mai puţin numeroase, dar extrem de importante, cum ar fi»Hi.imnca de dezinformare din timpul celui de-al Doilea Război Mnutllal, prin care Aliaţii i-au indus în eroare pe germani cu privire M h în alia debarcării din Normandia47.

«iperaţiunile de dezinformare pe timp de pace nu sunt extrem de». i inialnite, sunt mai puţin cunoscute şi uneori mai greu de depistat. IMuhe ecle mai spectaculoase astfel de operaţiuni putem menţiona m, i re a fost cunoscut sub numele „încredere", o organizaţie uivii iică părând ostilă noului regim comunist, dar care fusese, de «mi, înfiinţata şi condusă din 1921 până în 1927 de predecesorul h".. cunoscut sub numele CEKA48. Folosindu-se de acest fals grup în iipo/.iţie, sovieticii au intrat în contact cu

organizaţii anticomuniste ini uniate de emigranţi, precum şi cu serviciile de informaţii din i uiopa de Vest, reuşind astfel să prevină activităţile ostile pe care mevlea le-ar fi putut demara; au convins presupuşi opozanţi din I numea Sovietică să intre în contact cu organizaţia şi, astfel, CEKA în i putut afla identitatea; de asemenea, organizaţia a răspândit în nu a ţării informaţii false privind situaţia din interiorul Uniunii \nvictice49.

În anii ’50 şi la începutul anilor ’60, Uniunea Sovietică a declanşai lit puni de dezinformare menite să convingă Statele Unite că ea ileţiune mai multe resurse strategice nucleare decât avea de fapt. După, nu s-a menţionat mai devreme, în timpul unui zbor demonstrativ. Îi ocazia unei ceremonii organizate în luna iulie 1955, sovieticii au, etalat” 28 de bombardiere Bizon – probabil mai multe decât existau în inventarul propriu – prin crearea condiţiilor necesare pentru ca Inunul grup de avioane să iasă din raza vizuală a spectatorilor (inclusiv a reprezentantului forţelor aeriene americane) şi să revină pentru o a doua tură50. De asemenea, la sfârşitul anilor ’50, liderii sovietici, inspiraţi de prestigiul adus de succesul programului lor spaţial, au furnizat informaţi exagerate cu privire la programul ICBM al Uiüunii Sovietice51. Astfel, sovieticii au contribuit la accentua»* temerilor americanilor în ceea ce priveşte diferenţa uriaşa îl litiu bombardierele şi rachetele deţinute de ei şi cele ale Uniunii Sovleiltf (SUA se temeau că sovieticii aveau să le depăşească în ceea ce priveşte resursele nucleare strategice). Acţiunea de dezinformau Uniunii

Sovietice părea menită să convingă Occidentul să inel anumite concesii politice (de exemplu, în ceea ce priveşte stalului Berlinului) pe care, în mod normal, nu ar fi fost suficient de motivul să le facă52.

Conţinutul dezinformării – imaginea falsă pe care cineva don-ţi» să o creeze în ochii adversarului – depinde, desigur, de situaţie reacţiile aşteptate din partea adversarului. Pe timp de război, da exemplu, una dintre părţi ar putea dori să lanseze un atac-surpriel asupra inamicului şi, în acest caz, dezinformarea ar fi menită să îI convingă pe acesta că nu există iminenţa unui atac. În alte cazuri, cum ar fi debarcarea din Normandia, inamicul se aştepta să fii atacat, neexistând posibilitatea de a fi convins de contrariu. În acuM caz, dezinformarea are scopul de a convinge inamicul că atacul va avea loc în alt moment, loc sau mod decât cel plănuit.

Pe timp de pace, scopul dezinformării este mai puţin evident. Un stat ar putea dori să îşi convingă adversarul că este mai puternk decât în realitate sau să îl convingă să facă anumite concesii politice pe care altfel nu ar fi dispus să le facă. Sau, dimpotrivă, este posibil ca una dintre părţi să încerce să îşi disimuleze adevărata capacitate militară pentru a-şi linişti adversarul şi a-l determina să nu încerce, la rândul său, să îşi suplimenteze efectivele militare. Dacă forţele militare ale unui stat sunt limitate de un tratat privind controlul armelor, acesta ar putea urmări să ascundă încălcarea tratatului, obligând cealaltă parte să continue limitarea forţelor proprii.

Condiţiile necesare pentru succesul unei acţiuni de dezinformare

*Blocarea semnalelor reale şi fabricarea unora false*. Dacă ne imaginăm procesul de culegere a informaţiilor ca fiind receptarea şi interpretarea semnalelor emise de activităţile părţii supravegheate, atunci putem spune că operaţiunea de dezinformare implică, în măsura posibilului, blocarea semnalelor reale (cele care reflectă

În liniile reale) şi înlocuirea acestora cu unele menite să inducă în îi»mm Putem oferi un exemplu simplu: rezervorul din locaţia X hi» iiiuflat, iar în locaţia Y se află la vedere un rezervor fals din t»i itil prefabricat. Dacă un avion de recunoaştere inamic survolează fi«H.t ai putea trece cu vederea rezervorul din punctul X (deoarece Urnitului vizual este blocat de camuflaj) şi va raporta rezervorul din au» lui Y (cu condiţia ca semnalul emis de replica din prefabricat să îl» rtMinfinător cu unul real). În cazul operaţiunilor cu agenţi dubli, 4«h uinentele reale, de exemplu, vor rămâne în seiful guvernului iar»I«false, concepute special pentru operaţiunea de dezinformare, le «mi H livrate de agenţii dubli ofiţerilor lor de legătură.

I’i una parte a misiunii o reprezintă problemele legate de securitate. I Mi-a se transmit prea multe semnale reale, este posibil ca adversarul»4 nu mai fie indus în eroare, cu toate că amestecul de semnale false ti n-ale l-ar putea înşela, împiedicându-l astfel să îşi formeze o UMrttfine exactă a situaţiei. De aceea, una dintre

cele mai importante Miiiliii pentru o acţiune de dezinformare reuşită este abilitatea de a Mi h a majoritatea, dacă nu chiar toate canalele prin care adversarul 4» puica culege date. În general, acest lucru este mai uşor de realizat în timp de război decât pe timp de pace, fiind unul dintre motivele în uliu care acţiunile de dezinformare au mai multe şanse de reuşită în primul caz.

Pentru blocarea canalelor de culegere a informaţiilor este nevoie, în între altele, de cunoaşterea în detaliu a canalelor prin care adver

11 ul primeşte semnale. Este nevoie de resurse redutabile de intraspionaj, deoarece o sursă umană bine plasată ar putea dezvălui în iapa reală sau chiar planul de dezinformare. În plus, este nevoie în o bună cunoaştere a resurselor de culegere a informaţiilor prin mijloace tehnice pe care le deţine adversarul. Astfel, navele l»I ui aţele de zbor pot întrerupe orice tip de comunicaţii (de fapt, pot «lupta „controlul emisiilor" sau „emeon", deoarece undele radar... ui alte emisii electronice ar putea dezvălui poziţia vehiculului la fel le rapid ca şi transmisiunile radio) pentru a evita să fie detectate de Msiemele de interceptare inamice. Acelaşi efect ar putea fi obţinut şi în cazul forţelor terestre, dacă acestea s-ar folosi de linii terestre ti oniunicaţii prin telefon sau telegraf, cabluri optice etc.) în loc de unde radio, aşa cum au procedat germanii înaintea ofensivei din Ardem din decembrie 1944. De asemenea, dacă se cunosc orbitele sateliţilor de recunoaştere ai adversarilor, activităţile pot fi opilte i echipamentul camuflat sau mutat în locaţii

acoperite în mo în o ni y în care satelitul se află deasupra acestora, având posibilitatea de a t» fotografia.

O a doua componentă a misiunii, fabricarea unor semnale tal* se planifică tot ţinând cont de resursele deţinute de adversar prut»* culegerea informaţiilor prin mijloace tehnice. Agenţii dubli pl, transmite orice documente sau rapoarte false, atâta timp cât pol 4 explice cum au avut acces la acestea. Dezinformarea sistemei” tehnice de culegere a informaţiilor este mai complicată, dar poalhill Pentru a surprinde inamicul la Pearl Harbor, japonezii nu s-au lunile* la a impune flotei de atac încetarea comunicaţiilor pe perioade traversării Pacificului. În plus, alţi operatori navali de radio mm preocupat de transmiterea unor mesaje false unul către celfilalt, folosind semnalele flotei, dar cu transmiţătoare din Japonia. Am în dacă semnalele radio ar fi fost interceptate (deşi se pare că nu îţi fost) şi transmiţătoarele localizate, Statele Unite ar fi ajuns la COUcluzia că avioanele japoneze desfăşurau zboruri de exerciţiu la apele teritoriale53. În acelaşi mod, recunoaşterea fotografică poala fi păcălită, folosind replici ale armelor sau vehiculelor; pentru a afla cât de fidele trebuie să fie aceste copii ca să fie confundate cu cele reale, trebuie cunoscute capacităţile fotografice ale adversarului”.

Importanţa cunoaşterii resurselor pe care le deţine inamicul pentru a culege informaţii (canalele prin care îi parvine informaţia) este ilustrată de eşuarea planului britanic în timpul

celui de-al Doilea Război Mondial. În primele luni ale războiului, marina britanică a echipat trei nave comerciale cu arme false, pentru a le face să semene cu nave de luptă şi un portavion. Obiectivul era deturnarea atacurilor germane dinspre flota principală ancorată în portul Scapă Flow şi, în general, crearea confuziei printre germani cu privire la capacitatea reală a Marinei Regale. Cu toate acestea, varianta oficială a Serviciului britanic de contrainformaţii din timpul războiului era:

Din păcate, în această etapă a războiului nu exista altă metodă de a informa germanii asupra existenţei navelor decât prin expunerea acestora în faţa avioanelor de recunoaştere; iar Forţele Aeriene Germane nu păreau să le fi reperat. Nevoia de a sincroniza mai multe canale de dezinformare nu era încă suficient luată în considerare35.

*finibackul*. În desfăşurarea unei operaţiuni de dezinformare apar IwiMii.r.r incertitudini:

I Am losi blocate toate semnalele reale? f It Mimalele fabricate au ajuns la adversar? 1 A-raia a tras concluziile dorite?

În opul de a obţine răspunsuri la aceste întrebări, se pot folosi JmI multe metode pentru a afla modul în care adversarul evaluează»i i.1 Dacă nu este suficient de alert ca să observe semnalele false teu ilwc.1 nu le-a interpretat aşa cum ar fi dorit dezinformatorul, se în fain ca alte semnale pentru a-i atrage atenţia şi a-l conduce spre [khm pictarea dorită. Dacă începe să simtă că este ceva în neregulă cu inw Kinca (falsă) a situaţiei pe care

dezinformatorul i-a sugerat-o, se l*H nea noi semnale pentru a alunga orice urmă de îndoială. Dacă lveisarul a primit suficiente semnale reale pentru a-l ajuta să îşi Ni A o idee corectă asupra situaţiei, este recomandabil să se «liundoneze operaţiunea de dezinformare şi să se treacă la alt plan.

I eedbackul se poate obţine în mai multe feluri. În unele cazuri li nu ar fi dezirrformarea pe timp de război sau cea menită să susţină mi aiac-surpriză), acţiunile adversarului (sau lipsa acestora) ar putea fi Miliciente pentru a indica dacă operaţiunea de dezinformare am «ivit – Astfel, absenţa oricăror semne de intensificare a activităţilor militare (care s-ar fi putut observa foarte uşor) în cadrul flotei americane aflate la baza din Hawaii în prima săptămână a lunii unembrie 1941 le-ar fi oferit japonezilor toate informaţiile de care veau nevoie. În alte cazuri, pentru un feedback eficient ar putea fi nevoie de culegerea unor informaţii cu privire la atitudinea părţii hlverse faţă de situaţia dată; în cazul Sistemului încrucişat din timpul celui de-al Doilea Război Mondial, acest feedback a fost produs de interceptările Ultra, care le-au oferit britanicilor acces la eliberările înaltului Comandament german.

Cu cât este mai întinsă în timp şi mai minuţios planificată, le/informarea, cu atât e mai importantă obţinerea unui feedback «(icient. Partea dezinformată va reacţiona mai greu la astfel dele/informări şi, de aceea, trebuie să se găsească altă cale de a afla «Iacă momeala a fost

muşcată. În general, operaţiunile de dezin-lormare pe timp de pace necesită un feedback mai bun decât cele desfăşurate pe timp de război. În al doilea caz, este de aşteptat ca adversarul să acţioneze mai rapid, în funcţie de capacitatea ia à evaluarea a situaţiei reale, demonstrând astfel dacă a fost päc Allt timp de pace, adversarul este mai puţin presat să întreprindă al *m* ce ar putea dezvălui modul în care a procesat întreaga situaţi.

Acesta este unul dintre cele mai importante motive pentru i în operaţiunile de dezinformare sunt mai rar întâlnite pe timp de i decât pe tip de război. În plus, pe timp de război, este de aşteptai H victima unei operaţiuni de dezinformare să fie presată să réaction" rapid; astfel, are mai puţin timp pentru a analiza situaţia şi a coiu MMI semnalele primite pe diverse canale; de aceea, este de aşteptat H aceasta să fie mai uşor indus în eroare.

*Dezinformarea şi autodezinformarea*. O falsă percepţie aatthi atitudinii dorite din partea adversarului trebuie determinată de ac (la nile pe care le aşteptăm din partea acestuia. Cu toate acelea viziunea respectivă trebuie să pară plauzibilă; de fapt, este aşteptat ca scenariul de dezinformare să aibă succes dacă se ba/r a e «pe ceea ce adversarul presupune deja. De exemplu, dezinformaiM din Ziua Z a funcţionat atât de bine şi datorită faptului că Hitler oii deja convins că debarcarea Aliaţilor va avea loc la Calais, pe cea mai îngustă porţiune a Canalului Mânecii. Astfel, semnalele fabricate că avut numai rolul de a-i întări această convingere şi de a alunga ork t

urmă de îndoială ce ar fi putut surveni în urma eventualelor semnale reale ce s-ar fi putut scurge; aceasta este o misiune mai uşoară decât cea care presupune determinarea adversarului să adopte un între scenariu de dezinformare. De aceea nu este de mirare că succesele cele mai impresionante ale operaţiunilor de dezinformare implici elemente majore de autodezinformare.

Contradezinformarea

Din experienţă, putem afirma că este extrem de dificil să prevenim orice încercare de dezinformare din partea adversarilor. Chiar şi în perioada în care foloseau Sistemul încrucişat, britanicii erau înşelaţi în acelaşi mod de către germani cu privire la operaţiunile de tip gherilă şi cele de culegere a informaţiilor desfăşurate în Olanda. De la sfârşitul verii anului 1941, odată cu arestarea unui agent cir informaţii olandez care lucra pentru MI6, nemţii au reuşit să îi fihtiM pe toţi ceilalţi agenţi britanici trimişi în Olanda de către inimi de O peraţiuni Speciale (Special Operations Executive – SOE, în taim misiuni includeau sabotajul şi susţinerea grupărilor de ni-i antigermane). ilupa ce au descifrat sistemul codificat folosit de aceşti agenţi, pimmiii le-au trimis britanicilor mesaje ce păreau a veni din partea mp Im. care de fapt fuseseră arestaţi. Unii dintre agenţii arestaţi *ţa* tnliihurat la elaborarea şi transmiterea mesajelor; în alte cazuri îi tu Insi înlocuiţi cu operatori radio germani. Printre altele, cu h…1…111I acestor mesaje s-au făcut aranjamentele necesare pentru piMţiiiarca unor provizii suplimentare şi agenţi, care erau, de

fapt,» «tam ap imediat. Operaţiunea, denumită de germani *Nordpol* (Polul NIM tll şi *Englandspiel* (Meciul împotriva Angliei), a continuat până îi. l'M I. când doi dintre agenţii capturaţi au evadat din lagărul în *ţm* n-au închişi. În acel moment, imaginându-şi că vor fi oricum avu inspiraţi, conducerea serviciului militar german de contraln» tui mapi a decis să încheie acţiunea cu un mesaj simplu către Londra, ums în mod inspirat pe data de 1 aprilie56.

I inul dintre incidentele din cadrul acestei operaţiuni arată cât isti. (» puternică rezistenţa psihologică a unei persoane în faţa ideii el ml («ulm fi dezinformată. Atunci când agenţii britanici din Olanda millicau mesajele ce urmau a fi transmise către Londra, trebuia li im hula şi un „test de securitate" – o anume deviere (care ar fi pirul h simplă greşeală întâmplătoare) de la sistemul de cifrare, acciulă h»11 h indicat celor care primeau mesajul că ei chiar erau oiltt mi-ajucau că sunt şi că acţionau pe cont propriu, şi nu sub influenţa i în 1 manilor. De exemplu, să presupunem că un agent a fost instruit II Im.1 o „greşeală" la a cincisprezecea literă a fiecărui mesaj transmis. 1 Mi-a germanii ar fi obţinut sistemul de cifrare fără să înţeleagl în incipiul testului de securitate, orice mesaje trimise ar fi fost tratate 1 fiind false, din moment ce nu conţineau „eroarea" stabilită. În acest incident este vorba despre un operator radio german care h.msmitea mesaje în sistemul codificat obţinut de la un agent britanic «piurat. Deoarece operatorii radio pot fi uşor identificaţi după maniera în care

bat punctele şi liniile din codul Morse („stilul de 1 nere” sau „pumnul”), primul mesaj explica faptul că în Olanda fusese recrutat un nou operator, întrucât celălalt agent îşi luxase încheietura. Acest mesaj nu conţinea niciun test de securitate şi ar fi trebuit recunoscut de SOE ca fiind fals; de altfel, acesta INI. motivul pentru care testul de securitate fusese inventat. În hm.» ofiţerul de personal din Londra, deranjat de faptul că procedura în a fost respectată şi, evident, fără a ţine cont de motivul pentru Mtfţ procedura respectivă fusese instituită, a răspuns printr-un ordin ca n»a operator radio „să fie instruit cum să folosească testul de securitate în orice caz, primul pas spre evitarea dezinformării este înţelegerii modului cum funcţionează aceasta; după înţelegerea factorilor t ale facilitează dezinformarea, cel puţin se poate prevedea posibilltalel de a fi victima unei dezinformări şi recunoaşte câteva semnale de avertizare. O persoană este cu atât mai vulnerabilă în faţa doiln formării dacă se bazează pe un număr mic de canale de informare *v* dacă adversarul e la curent cu natura acestor canale şi modalitatea lor de operare.

De exemplu, folosirea excesivă a sateliţilor de recunoaştere folii grafică, ale căror identitate şi orbite vor fi cunoscute mai devreme sau mai târziu de către cei fotografiaţi, creşte vulnerabilitatea în laa operaţiunilor de dezinformare. Cunoscând momentele în care locaţiile sale pot fi fotografiate, adversarul se poate asigura îi anumite lucruri nu sunt observate: obiectele respective ar putea îl

mutate în garaje sau hambare ori acoperite cu echipament de camu flaj de fiecare dată când un satelit de recunoaştere trece pe deasupra zonei respective. De asemenea, adversarul ştie când este momentul să expună echipamente false pentru a spori şansele ca acestea să fie observate şi confundate cu cele reale.

Situaţia este evident mai gravă (din punctul de vedere al poteriţialei victime a operaţiunii de dezinformare) dacă adversarul poate afla din timp nu doar locaţiile ce pot fi fotografiate, ci şi care dintre acestea *vor fi* fotografiate. De asemenea, este şi mai grav daci adversarul cunoaşte performanţele exacte ale satelitului. De exemplu, în cazul în care cunoaşte rezoluţia satelitului, va şti cât de fidelfl trebuie să fie copia echipamentului pentru a părea identică. De aceea, sovieticii au dat o lovitură de maestru când au reuşit să intre în posesia cărţii tehnice a satelitului american de recunoaştere fotografică KH-11. L-au cumpărat în schimbul a numai trei mii de dolari de la William Kamplies, după ce acesta a demisionat din poziţia de ofiţer inferior CIA în noiembrie 197758. De aceea, foto grafiile din satelit (care ar putea indica exact ce detalii pot li identificate) sunt strict secrete. (Dacă este necesar ca fotografiile din utili unlie făcute publice, calitatea acestora trebuie deteriorată PMIM n nu dezvălui performanţele exacte ale sistemului.) t am ce au fost înţelese riscurile implicate de folosirea unui singur de informare, se pot lua măsurile necesare. Cea mai bună soluţie f H Întinderea operaţiunilor denumite şi „culegeri neaşteptate”, adică

Hpiidierea la ore şi în locuri pe care adversarul nu le poate anticipa. i-iiuu este mai greu de realizat acest lucru în cazul recunoaşterii pin utlelit, din cauza faptului că orbitele sunt previzibile; operaţiunea pnaie realiza mai uşor de-a lungul graniţelor sau coastelor»tMitirului inamic, acolo unde este posibilă fotografierea aeriană.

În toate acestea, se pot urma anumiţi paşi chiar şi în cazul Motu îi sateliţilor. Deşi adversarul ar putea avea capacitatea (prin huliriea orbitelor, de exemplu) de a determina care sateliţi desfă

Îi acţiuni de recunoaştere, acest lucru necesită timp şi va dura mi va reuşi să transmită semnalul de alarmă în bazele sale militare. Im ţii unele ore de zbor ale satelitului sunt mai multe şanse ca Miujiufiile să fie făcute pe nepregătite. De aceea este bine să se mliilească cu atenţie ce locaţii vor fi fotografiate la prima trecere a mii Inului. De asemenea, se va acorda o atenţie deosebită modalităţilor im care se poate prelungi perioada în care fotografiile se fac pe» luegiitite, prin modificarea caracteristicilor de lansare şi deplasare «li sateliţilor, astfel încât adversarul să îi depisteze mai greu59. De «temenea, dacă s-ar găsi modalitatea în care să se lanseze pe orbită mal mulţi sateliţi de recunoaştere în acelaşi timp (poate chiar şi falşi mirliţi pe care adversarul să nu îi poată deosebi de cei reali), este puţinii ca adversarul să nu îşi mai poată proteja echipamentele şi, lumile militare fără să îi fie serios afectate operaţiunile.

111 schimb, mulţi susţinători ai culegerii de informaţii din comunicaţii h preferă pe aceasta

faţă de celelalte metode, deoarece mai mulţi l-ai lori garantează veridicitatea informaţiilor culese. Culegerea informaţiilor din comunicaţii (*comint*) se poate face la scară mult mai mate, crescând astfel şansele de a capta semnalele reale. De e.cinenea, ar fi nevoie de un efort mult mai mare pentru a dezinforma 11 *mint* printr-o reţea radio falsă (caz în care ar trebui folosite resurse i personal pentru a fabrica semnalele), spre deosebire de cazurile în ne ar fi nevoie să se expună echipamente false sau să se recruteze i să se folosească un agent dublu60.

liste şi mai important faptul că adversarul nu va putea stabili cu «\actitate ce canale de comunicaţii îi sunt interceptate; de aceea este posibil să trimită mesaje false care nu vor fi niciodată interceptat» le timp ce unele dintre cele reale ar putea fi. Însă nici această soluţie nu m* imbatabilă; spionajul (cum a fost cazul lui Geoffrey Prime, luiyajiH Agenţiei Naţionale de Comunicaţii [GCHQ], echivalentul Iuii, nu g Agenţiei Naţionale de Securitate [NSA] din SUA) şi anumite tuil»t*«tehnice ar putea ajuta adversarul să identifice frecvenţele sau Hull!» è comunicaţii pe care ceilalţi le interceptează61. În acest caz, canalul» A comunicaţii pot fi folosite pentru operaţiuni de dezinformare.

O situaţie complicată de acest gen a avut loc în 1953IVII *ţ* ilustrează dificultatea evaluării posibilelor operaţiuni de delii formare. Statele Unite şi Marea Britanie au săpat în Berlin un IMN din zona controlată de americani până în cea controlată de i tot pentru a instala dispozitive de

interceptare pe mai multe linii telefbnfre şi telegrafice ce asigurau legătura între oraş şi comandamentul forţelor aeriene din Karlshorst. Tunelul a fost construit prinţi îl efort comun al MI6 şi CIA. Din nefericire, George Blake, ofle) superior al MI6 detaşat la Berlin, era de fapt spion sovietic. (A hm deconspirat în cele din urmă, arestat şi condamnat în 1961.) Blitke participat la una dintre primele întâlniri la care s-au plani ht et chestiuni legate de tunel şi i-a informat pe ruşi62.

Oricum, cele mai importante comunicate telegrafice transmite de ruşi pe liniile interceptate erau codificate. Potrivit lui John Ranelagh, care, în relatările sale despre istoria CIA, pare să te bazeze pe numeroase informaţii obţinute de la foştii ofiţeri, adevăratul secret al operaţiunii era existenţa unei tehnici ce permite* CIA să recupereze integral textul mesajelor criptate63. Britanicii nu ştiau despre această tehnică şi, de aceea, era imposibil ca Blake să fi dat detalii despre ea. Astfel, deşi fuseseră informaţi despre dispo zitivele de interceptare, sovieticii ar fi putut continua să folosească linia telegrafică pentru mesajele importante, fiind convinşi că metodele de criptare garantau siguranţa comunicaţiilor.

Şi britanicii au avut rolul lor în culegerea informaţiilor prin operaţiunea tunelul din Berlin. Potrivit lui Ranelagh, „trebuia ca britanicii să efectueze analiza a jumătate dintre materialele rezultate”1 Dacă acest lucru se întâmpla, ar fi fost evident că Statele Unite aveau o metodă de interpretare a mesajelor interceptate; dacă Blake ar fi aflat acest detaliu, sovieticii ar fi realizat că

tunelul reprezenta o problemă majoră.

I»(M itiiuinea tunelul s-a finalizat pe 21 aprilie 1956, la aproape un şi ilintă i e a fost interceptat primul mesaj, după ce se pare că ar fi e cu uWoperit de sovietici în timpul unor reparaţii la unul dintre hMmi de pe care se montaseră dispozitive de interceptare. La momentul t*«nv CIA, neştiind despre existenţa unui spion sovietic în biroul» în ihn herlin, a considerat descoperirea sovieticilor ca fiind acci-êtfetifl Acum, desigur, putem lua în considerare posibilitatea ca sovieticii M fi jacul descoperirea" intenţionat pentru a-l proteja pe Blake.

! nif interesant de analizat în ce măsură „captura" din această»Milunc poate fi privită ca dezinformare. Pe de o parte, este, mm/ilul ca sovieticii să fi aflat repede despre operaţiune de la flUU, faptul că nu au intervenit ar putea sugera că se foloseau de i.hipr pentru a dezinforma Statele Unite şi Marea Britanie Pe de unt parte, sovieticii erau nevoiţi să îşi protejeze sursa; dacă ar fi «Ilouai imediat pentru închiderea tunelului sau pentru modificarea o wiilui comunicaţiilor, ar fi riscat să alerteze Statele Unite şi Marea Miiianie în legătură cu posibilitatea existenţei unui trădător. De «m. menea, dacă ar fi avertizat mai mulţi ofiţeri că liniile respective mi h au sigure, riscau ca Statele Unite şi Marea Britanie să afle că v inicii ştiau despre tunel.

Iu orice caz, ar trebui analizate cu atenţie informaţiile rezultate în h mă operaţiunii; informaţiile valoroase ar indica o probabilitate mai îi n/ulă ca sovieticii să fi conştientizat faptul că

linia nu era sigură i Itauelagb susţine că primele indicii despre existenţa unui agent sovietic lui «adrul MI6 ar fi fost obţinute în urma operaţiunii tunelul) 65. Ar fi în provocare încercarea de a afla dacă sovieticii ştiau de operaţiune înainte de descoperirea lor aparent întâmplătoare şi, dacă da, când".

Chiar şi în absenţa unor indicii conform cărora inamicul ar inUTcepta o anumită linie de comunicaţii, pentru dezinformare se putea crea o întreagă reţea de transmitere radio, cu unicul scop de a îi aromite mesaje care să fie interceptate de inamic; dacă reţeaua e le suficient de mare, inamicul se va lovi de ea mai devreme sau mai târziu. Aceasta ar fi o măsură costisitoare şi complicată; însă pe nmp de război este posibil de realizat. Înaintea debarcării din Ziua Z, Matele Unite şi Marea Britanie au creat o asemenea reţea radio pentru a-i convinge pe germani că exista un grup armat al Statelor Huite, staţionat în Sud-Estul Angliei şi pregătit să pornească adevăratul" atac asupra zonei Calais. De fapt, grupul armat era format numai din câţiva soldaţi adevăraţi şi „comandam George S. Patton Jr.; cea mai mare parte a divizioanelor şi celui i componente existau numai pe hârtie şi în discuţiile radio pui la între operatorii reţelei false.

Acesta a fost un element important al operaţiunii de dezinformate din Ziua Z; operaţiunea nu numai că a ajutat la mascarea debarc ftt îl ci i-a determinat pe germani să nu detaşeze trupe suplimentai? ta Normandia în zilele cruciale ce au urmat debarcării. Germanii **

interpretat operaţiunile din Normandia ca fiind o diversiune, a modalitate de a le distrage atenţia de la invazia ce avea să urinau Conform unui studiu asupra operaţiunilor de dezinformare din timpul celui de-al Doilea Război Mondial:

Reţelele folosite pentru comunicaţiile radio false erau extrem de mi inşi complicate. La vâri se aflau 22 de formaţiuni false [presupun, i. comandamente, precum şi armatele şi divizioanele componente]... Este aproape sigur că tocmai acest trafic radio simulat, din care cea turnare parte s-a desfăşurat la distanţă mică de inamic şi care a fost uv de monitorizat, a fost cel mai important factor al operaţiunii it* dezinformare, cu excepţia agenţilor dubli67.

Aceiaşi factori ne pot ajuta să depistăm pericolul de dezinformai» prin culegerea unor informaţii *humint*. Atunci când culegerea intuimaţiilor din surse umane se bazează excesiv pe dezertori, creşle considerabil posibilitatea de dezinformare. În primul rând, spre deosebire de cazul în care există un agent infiltrat, inamicul cunoaşte identitatea dezertorului şi poate stabili cu aproximaţie la ce fel de informaţii a avut acesta acces. Inamicul nu poate împiedica dezertorul să spună ceea ce ştie, dar poate ţine cont de datele respective într-o operaţiune de dezinformare. De aceea, informaliile primite de la un dezertor sunt asemănătoare cu „culegerea anticipată".

În al doilea rând, adversarul poate infiltra cu uşurinţă un dezertoi care să furnizeze date false menite să dezinformeze. În cazul în care se folosesc excesiv dezertorii, inamicul ar putea pune

la dispoziţie mal mulţi, ale căror rapoarte, deşi false, să se confirme reciproc. Ca urmare a suspiciunilor că, încă de la începutul anilor ’60, Uniunea Sovieticii ar fi procedat astfel faţă de Statele Unite, în 1970 au avut loc unele dintre cele mai grave conflicte interne din istoria CIA, între cei care luau această posibilitate în serios şi cei ce o considerau deplasată vmM.» ilm urmă au câştigat în cele din urmă, când James Angleton, p-ţi Imnului de contrainformaţii CIA şi cel mai fervent susţinător al ff-uH vi/luni, a fost concediat de William Colby în decembrie 197468.

Analiza contrainformativă

4 t* i tun am demonstrat prin discuţia privind agenţii dubli şi é»mini marea, protejarea integrităţii operaţiunilor de culegere a frifuiiituţiilor este foarte greu de realizat şi implică mult mai multe fiMurnic decât deconspirarea spionilor. De fapt, este posibil ca mai Mtulir e uzuri să fie legate între ele; pentru protejarea sistemului de ilt une a datelor împotriva infiltrărilor şi dezinformării este nevoie h un birou special de analiză contrainformativă care să joace rolul fa memorie a instituţiei şi să analizeze toate aceste conexiuni. 1 nu mai bună modalitate de a determina dacă sistemul de culegere i mii hmaţiilor a fost penetrat este de a avea acces la o sursă la nivel în il! din serviciul advers (fie un agent în activitate, fie un defector). iii.u şi aşa, ar fi o chestiune de noroc dacă sursa respectivă ar putea nli muica spionii după nume. Acest lucru ar fi posibil numai dacă Éuun ar fi direct implicată în dirijarea lor sau ar fi un ofiţer

de rang i»mii le înalt din serviciul advers. Cel mai probabil, sursa va putea îi i i indicii privind identitatea spionilor. Pentru a obţine rezultate în Mima acestor indicii, va fi nevoie de un efort analitic.

De exemplu, este posibil să se descopere că inamicul a avut acces îi mai multe documente clasificate privind un anumit subiect, i în Mipunând că informaţiile au provenit de la un singur agent, se (Miale revizui lista de distribuire a documentelor compromise şi să i ale stabili ce oficiali au avut acces la toate acestea. Este posibil şi ursa să ştie că spionul a avut o întâlnire cu coordonatorul său iun un anumit oraş din străinătate, la o anumită dată. Informaţiile li raie de călătorie pot să indice ce oficiali, dintre cei care au acces i. informaţii deosebite, au fost în oraşul respectiv la data aceea.

În plus, se pot folosi şi alte indicii care sugerează penetrări de h în e fel ale sistemului. Astfel, dacă o operaţiune eşuează (un agent le descoperit sau un sistem tehnic de culegere a informaţiilor e – Hiipromis) într-un mod care sugerează că adversarul avea cunoştinţă de operaţiune înainte ca aceasta să aibă loc, trebuie Invethap modalităţile în care a putut afla detaliile. Se vor descopeti fi o îndoială, multe canale prin care informaţia ar fi putut aune inamic (indivizi cu acces la informaţii sau vulnerabilităţi ori Mi * * securitate). Dacă însă există o serie de astfel de eşecuri, te pl, reduce pistele de investigaţie; spre exemplu, este posibil t * 9 singur individ să fi avut acces la toate informaţiile. În schimb. În multe

eşecuri consecutive pot indica şi faptul că a fost compromit în canal sau sistem de comunicaţii. De exemplu, de la sfârşitul «itilM 60 până la începutul anilor ’80, oficialii marinei Statelor Unite et fost surprinşi să întâlnească de mai multe ori nave sovietic*»t aşteptau navele de război americane în zone care fuseseră alem îl secret ca spaţiu de exerciţiu.

„Este ca şi cum ar fi avut o copie a planurilor operaţiunilor*, t declarat un amiral. Dar Statele Unite au aflat că documentele refttltoare la cifrul naval le-au fost transmise în mod regulat sovietielkl numai după ce a fost descoperită reţeaua de spionaj al lui Iuta Walker în 1985 şi deci este posibil ca volumul mare al traficului de mesaje navale cifrate să fi fost citit de către aceştia69. În orice c-au» a astfel de înlănţuire a evenimentelor ar trebui să alerteze un servitla de informaţii privind posibilitatea ca adversarul său să aibă résulte umane sau tehnice eficiente pentru culegerea informaţiilor, cate trebuie descoperite şi neutralizate.

Un caz asemănător este şi acela al trădării lui Aldridge Aniet, care a dus la pierderea unui număr important de surse de informaţii din Uniunea Sovietică în perioada 1985 – 1986, când CIA a fost alertait referitor la existenţa unei grave probleme70. La început, CIA a bănuit că i-au fost interceptate comunicaţiile de către KGB sau că anumite cazuri au fost prost coordonate (de exemplu, că expertiza nu a toţi corespunzătoare, oferindu-le sovieticilor ocazia de a le identifica) ţi, că „fiecare caz ar fi putut însemna «începutul

sfârşitului» acestuia” 7

Demersurile ulterioare ale CIA pentru a găsi cauza acestot pierderi au fost împiedicate de o sumă de factori: operaţiuni de dezinformare ale KGB, cazul Lonetree, şi suspiciunile că sovieticii au plantat microfoane în Ambasada Statelor Unite din Moscova72. În cele din urmă, CIA şi-a îndreptat atenţia asupra lui Ames nu datorită analizei contrainformative în legătură cu pierderile suferite, ci faptului că un coleg al său a observat şi a raportat că Ames avea un stil de viaţă care depăşea mijloacele financiare de care dispunea73.

Capitolul 6

Controlul paznicilor: managementul culegerii informaţiilor i de patru capitole anterioare au abordat tipurile de activităţi de»I. jteic a informaţiilor şi unele aspecte referitoare la acestea. În amnare ne vom îndrepta atenţia asupra relaţiei dintre serviciile de ammaţii şi autorităţile guvernamentale căreia i se subordonează, – Mim şi asupra chestiunilor legate de managementul culegerii minunăţiilor din perspectiva superiorilor ce nu fac parte din serviili de informaţii sau „a stăpânilor politici”.

Din punct de vedere managerial (sau al administraţiei publice), u.numaţiile prezintă două seturi de probleme importante. Primul set i. Îi va din caracterul secret specific activităţii informative; acesta în m vedere dificultăţile speciale legate de caracterul secret, pe care h miampină factorii politici cu responsabilităţi în supravegherea şi miiolul activităţilor informative.

Al doilea set derivă din incom-iMiihilitatea dintre expertiză şi procesul de luare a deciziilor. Se referă i» pl, ol»lemele privind atribuirea importanţei cuvenite opiniilor experţilor». ale susţin că posedă cunoştinţe speciale) care se ocupă de consilierea i îi lorilor de decizie (care au de fapt autoritatea de a lua decizii).

Caracterul secret şi controlul

I un-un guvern modern, cu mii de angajaţi implicaţi în structuri lui ocratice complexe, problema controlării numeroaselor lor activităţi şi a verificării conformităţii acestora cu legile şi politicile adoptate de superiori este foarte dificilă. În ceea ce priveşte agnum de informaţii, problema principală constă în caracterul am»M § activităţii lor, oricât de legitimă ar fi necesitatea de a litte *mm* anumite surse de informare, metode şi activităţi, dar şi în cu mrţionarea accesului la aceste informaţii la un număr cât mai mi» oficiali din guvern.

Desigur că, în principiu, controlul activităţilor guvernamental este organizat într-un mod ierarhic, astfel încât fiecare oficial efli răspunzător în cele din urmă, prin lanţul de comandă, în faţa eh-ţi guvernului. Astfel, condiţia minimă a controlului este ca flehen superior să aibă dreptul de a cunoaşte toate informaţiile la care în acces subordonaţii săi. În general, această condiţie este întinau* deşi noţiunea de *negare plauzibilă* pune unele semne de între importante în această privinţă.

Accesul teoretic la informaţii privind o anumită activitate nu et* totuşi acelaşi lucru cu

faptul de a avea suficiente cunoştinţe penitii t o controla într-un mod eficient. În alte domenii de activitate guverna mentală, controlul ierarhic direct, exercitat de către superiori, ettt suplimentat prin alte mecanisme, atât oficiale, cât şi neoficiale inspecţii ale auditorilor sau ale inspectorilor generali, contestări l plângeri referitoare la birocraţie, venite din partea unor părţi advet te investigaţii efectuate de agenţiile responsabile de aplicarea Icnii supraveghere legislativă, mediatizare şi reclamaţii sau alte tipuri «îl* reacţii ale publicului.

Aplicarea acestor mecanisme în activităţile informative necealH aducerea lor la cunoştinţa unui număr mai mare de persoane, cate depăşeşte cercul de oficiali a căror necesitate de a fi informaţi derivi din implicarea lor concretă în astfel de activităţi. Cât de mare ai trebui să fie numărul de persoane informate depinde de mecanismele respective, întrucât unul dintre ele poate presupune informarea doar a câtorva oficiali din ramurile executive, altul implică informarea membrilor organelor legislative şi a cabinetelor acestora, iar un al treilea publicul larg. În fiecare dintre cazuri, trebuie să se ajungă la un echilibru între riscul inerent lărgirii cercului celor cu acces la informaţii, pe de o parte, şi beneficiul care derivă din capacitatea mărită a superiorilor politici ai agenţiilor de informaţii de a controla activitatea acestora, pe de altă parte.

I ihm plauzibilă

— «-o ai toate mecanismele de control implică o mai mare diseminare llhfi imuiiilor, se poate

spune că, în general, există o tensiune între ştntiitul secret şi controlul eficient. Totuşi, în ceea ce priveşte e iivun (de informative, realizarea unui control eficient poate fi ihmiţilk ăla şi mai mult de doctrina negării plauzibile, care sugerează îl îi nu control ierarhic fundamental al superiorilor poate fi pus la inimialn. Conform acestei doctrine, după cum am menţionat şi mai hm activităţile informative care ar putea duce la complicaţii (din i u/a faptului că încalcă legislaţia internaţională sau din orice alt inimiiv) ar trebui să fie planificate şi executate astfel încât şeful juvemului să poată nega credibil că ar fi avut vreo legătură cu 4 i în ea sau chiar că ar fi avut cunoştinţă despre faptul că ele au avut Im După cum am precizat, această doctrină este asociată de obicei. a ficţiunile secrete, deşi se poate aplica şi altor activităţi informative.

* nu ar fi spionajul sau recunoaşterea fotografică aeriană, care violează spaţiul aerian al ţintei.

Negarea plauzibilă poate să complice controlul activităţilor Informative cărora li se aplică. Pentru a fi eficientă, nu numai că im teşită limitarea cunoaşterii activităţii la cel mai mic număr posibil «le oficiali, ci presupune şi absenţa unei proceduri oficiale de aprohuie, dar şi a documentelor în care să se înregistreze respectiva upiobare. Activitatea însăşi ar trebui derulată astfel încât volumul, valenţelor să fie redus la minim, iar după finalizarea activităţii, juobabil că ar trebui distruse orice documente create. Evident că tisilel se creează condiţiile unor neînţelegeri şi

a unei incertitudini cu în ivire la autorizarea unei anumite acţiuni. În special, fără o evidenţă în lisă, ar fi imposibil să se stabilească dacă o astfel de activitate a fost aprobată de către şeful guvernului sau de un alt oficial de rang malt care nu aparţine domeniului informaţiilor.

Toate acestea nu înseamnă că vreuna dintre agenţiile de informaţii este „un element ostil”, ca să citǎm o expresie atribuită senatorului 1 rank Church1. Cu condiţia ca situaţia să nu se schimbe, o agenţie de informaţii poate „sări gardul” mult mai uşor decât orice alte organizaţii guvernamentale. Împotriva acestei imixtiuni, trebuie totuşi precizat că agenţiile de informaţi investighează caracterul potenţialilor angajaţi mai atent decât o fac alte birouri guvernamentale şi posibilitatea dobândirii unor avantaje materiale ilicite în cadrul une* agenţii de informaţii este mai mică decât în multe alte bine guvernamentale, cum ar fi cele care se ocupă cu statistici 9I nottn economice sau care fac afaceri în numele guvernului – de exonttlu prin atribuirea unor contracte sau prin închirierea terenurilor altele în proprietatea guvernului spre exploatare privată.

Poate cel mai uimitor exemplu care ilustrează cum funcţioneai în practică, negarea plauzibilă a fost oferit de investigaţia efectuat! de Congres în 1975 – 1976 asupra activităţilor informative ale Statal” Unite. O comisie a Senatului, condusă de către senatorul Chutvti (cunoscută înainte sub denumirea Comisia Specială a Senatului pentru studiul operaţiunilor guvernamentale referitoare la activităţl Ni informative) a examinat tentativele

CIA de a-l asasina pe liderul cubanez Fidel Castro la începutul anilor ’60. Conform raportului comisiei privind implicarea CIA în planurile secrete de asasinate, „au fost dovezi insuficiente din care Comisia să poată trage conduita că preşedinţii Eisenhower, Kennedy sau Johnson, consilierii apropia”, ai acestora sau Grupul Special [grupul interagenţii ce revizuia propu nerile de acţiuni secrete] au autorizat asasinarea lui Castro” 2.

De fapt, dosarul găsit de comisie era uimitor de vag în ceea le priveşte autorizarea. Oficialii importanţi ai CIA au declarat est ei s-au considerat autorizaţi în totalitate pentru a face ceea ce au făcut, dar că această autorizare nu a fost transmisă în atât de multe cuvinte, nici oral, nici în scris. Pe scurt, comisia a examinat cu atenlle documentele sau, mai precis, lipsa acestora, la care te puteai aştepta într-o situaţie în care doctrina negării plauzibile era predominanta Nimic din dosarul disponibil nu l-ar fi împiedicat pe preşedintele John F. Kennedy sau pe fratele acestuia, procurorul general Robett F. Kennedy (care a jucat un rol important în elaborarea strategiei politice faţă de Cuba), să nege în mod plauzibil orice implicare sau cunoştinţă despre tentativele de asasinat3.

Astfel, în ciuda unei dispute *a priori* privind dificultatea exercitării controlului asupra agenţiilor de informaţii, raportul Comisiei Church nu arată concret că acelaşi lucru s-a aplicat şi în privinţa tentativeloi de a-l asasina pe Castro. Mai degrabă demonstrează cum ar funcţiona doctrina

negării plauzibile pentru a proteja preşedintele de asumarea responsabilităţii. Astfel, inevitabil, rămâne valabilă posibilitatea că tă hi h scăpat de sub control, dar pare improbabil că chiar aşa a

Nniru cine lucrează serviciile de informaţii?

m i (*v* caz, este ciudat ca un şef de guvern să îşi exercite atribuţiile Ut Minimi în concordanţă cu doctrina negării plauzibile. Nu se hMtunuă deloc cu controlul obişnuit, pe care şeful guvernului îl *nu* HA asupra departamentelor sau ministerelor prin lanţul de MHiumdă oficial şi prin ordine scrise, hotărâri de guvern, declaraţii l-iililic\ memorandumuri şi aşa mai departe. Baza acestuia constă mal degrabă într-o loialitate directă sau personală a serviciului de minimalii faţă de şeful guvernului decât într-o subordonare birocratică.

În ireçut, serviciile de informaţii lucrau de obicei pentru un mm îi. Îi h, un ministru-şef sau un comandant suprem, în afara structurilor (Msi i na mentale obişnuite. De exemplu, Sir Francis Walsingham, îi iliiibilul secretar de stat al Reginei Elisabeta I a Angliei, a finanţat ui m-i viciu de informaţii foarte eficient, în mare parte, din propriile Muluri (şi aproape a dat faliment din această cauză) 5. În mod ««mănător, ducele de Marlborough, comandantul suprem britanic ilm timpul Războiului de Secesiune din Spania, a folosit o taxă de % pe salariile plătite de britanici pentru trupele străine din armata ia, ca şi alte câştiguri suplimentare (sau tradiţionala mită, ca să h «h istm un limbaj mai puţin elegant), provenite din diverse contracte îi achiziţii, pentru a finanţa un serviciu secret cu un succes aparent.

I l.1 considerat că aceste fonduri au fost cheltuite în mod adecvat ci utru „a procura informaţii şi alte servicii secrete”, dar ulterior a inşi pus sub urmărire penală de către oponenţii săi politici pentru tli Miirnare de fonduri6. În ambele cazuri, distincţia dintre fonduri sau îi nvităţi publice şi cele private era neclară. Evident că un astfel de tunjament nu poate fi tolerat foarte uşor de un stat birocratic modern, în care separarea între îndatoririle publice ale oficialilor şi interesele lor private se presupune că este absolută7.

Dar această problemă depăşeşte asigurarea răspunderii pentru i» îndurile publice. Problema şi mai importantă este cine poate autoriza l»r oricine altcineva să se angajeze în astfel de activităţi. Acest aspect «.ic foarte important într-o guvernare constituţională, precum cea a Matelor Unite, în care puterea executivă este împărţită între departamentele guvernamentale, iar demnitarii răspund în fraţii «te toratului. Preşedintele îşi arogă dreptul de a autoriza derularea im*«operaţiuni informative, pe baza politicii sale externe şi a roi-e stabilităţilor militare conferite de Constituţie. În acelaşi timp, dupt cum am discutat în capitolul 4, referitor la acţiunile sceri MÉT Congresul a insistat asupra unui circuit complet al documeti! hH care să facă legătura între activităţile informative şi cei ce le autorizat. Astfel, un efect important al implicării Congresului în acest domeniu a fost subordonarea activităţilor informative CIN trolului birocratic din cadrul ramurii executive.

Dar implicarea Congresului a depăşit şi problema autorizării t controlării activităţilor informative de către ramura executtvi Comisiile de informaţii din Camera Reprezentanţilor şi Senul Mi subliniat cu succes dreptul de a fi „informate complet şi în nun» regulat cu privire la activităţile informative” şi de a primi „oprit* date... cu privire la activităţile informative pe care le desfăşonrl” oricare agenţie de informaţii8. Coroborat cu revigorata „putem capitalului” (puterea Congresului de a-şi însuşi fonduri sau de reţine fonduri pentru informaţii, ca şi pentru toate celelalte activlt Ăţi, guvernamentale), Congresul putea folosi – şi, într-o anumită măsuri, a şi făcut-o –, aceste mijloace persuasive pentru a stabili o autorii»!» asupra informaţiilor, împreună cu preşedintele.

Rezultatul, după cum se exprima un fost director al CIA, Robeti M. Gates:

...constă în faptul că astăzi CIA a ajuns într-o poziţie remarcabili, echilibrată involuntar, aproape echidistant, între ramurile executiva l legislativă. Administraţia ştie că CIA nu se află în poziţia de a ascunde Congresului informaţii şi că este extrem de sensibilă la cererile lui, Congresul are o influenţă enormă şi multe informaţii, rămâne suspiciu* şi neîncrezător9.

Această discuţie privind implicarea Congresului în aspecte ce [\\ de culegerea informaţiilor ajută la explicarea altei probleme de control: astfel de controale nu vor da impresia organului legislativ că îşi exercită în mod eficient autoritatea asupra serviciului, oricui de oportun

consideră şeful guvernului că este caracterul neoficial al controlului unui serviciu de informaţii. Din această cauză suni necesare mai multe mijloace de control, cum ar fi cele deja menţionauümiii oficial la informaţii, notificări privind anumite tipuri de îi m şi cerinţa ca fondurile pentru activităţile informative să fie lÉintuc prin lege). Astfel, în Statele Unite, rezultatul implicării lungirnului a fost că CIA şi alte agenţii de informaţii au fost fult Midonate controlului total al executivului şi aceluiaşi sistem de iituliol parlamentar ca şi orice alt departament al guvernului, i Îimllunea controlului parlamentar va fi abordată ulterior în acest râutiol, în legătură cu discutarea relaţiei dintre serviciile de infor-*4) ÎI şi democraţie.

Npertiză şi strategie

».» punea anterioară a făcut referire la relaţia dintre nevoia de a i. tlAşura activităţi în secret şi managementul activităţilor informative, i h.di set de probleme implică relaţia dificilă dintre expertiză şi iniirgic – adică dintre cei care au cunoştinţe de specialitate refemre la o problemă şi cei ce sunt autorizaţi să stabilească şi să implementeze politica guvernului referitoare la ea. Această relaţie Mimiituie o problemă în cadrul celorlalte departamente ale guvernului, indiferent de regiunile politice pe care le acoperă, fiind este o f. uia frecvent abordată de reprezentanţii administraţiei publice.

Multe probleme şi contradicţii apar de obicei între expertiză şi iiiaiegie. Importantă este problema rolului pe care expertiza îl poate mi în

procesul luării deciziilor. Unde ar trebui trasă linia între funcţiile şi responsabilităţile experţilor, pe de o parte, şi cele ale Im lorilor de decizie, pe de altă parte? Evident că vrem ca strategia»filie construită pe baza celor mai bune informaţii disponibile; am» ondamna un factor de decizie care ar ignora faptele puse la dispo-n pe şi şi-ar baza acţiunile pe propriile păreri nejustificate despre Iunie. În acelaşi timp, vrem ca strategia politică să fie stabilită de cei nora sistemul politic (prin alegere sau numire) le-a acordat unoritatea de a conduce; în orice caz, aceştia trebuie să-şi asume m”» i) onsabilitatea pentru strategiile promovate, fără a ţine cont de informaţiile pe care s-au bazat ele.

Ştiinţele sociale contemporane rezolvă teoretic această problemă în intermediul distincţiei „fapt/valoare”: ştiinţele sociale pot oferi fapte (inclusiv pronosticuri arbitrare, cum ar fi: „Dacă guvtMHnt urmează politica Xi va obţine rezultatul Yj”), dar factorii de dfMife deţin monopolul alegerii obiectivelor ce trebuie urmărite i*U. i preferă rezultatul *Y*{ rezultatului Y2 sau viceversa).

Această soluţie teoretică oferă totuşi foarte puţine îndrumtH practice. În primul rând, ştiinţele sociale sunt departe de a rettl i facă pronosticuri arbitrare, în majoritatea domeniilor; desigur el, t» ceea ce priveşte problemele de securitate naţională de care se în serviciile de informaţii, acest tip de abilitate predictivă nu NU disponibilă. În al doilea rând, dezbaterile pe tema securitiţM naţionale se ocupă mai mult cu diferite evaluări

ale strategul” aplicate şi mai puţin cu dezacordurile referitoare la obiectivele i’ Aft ar trebui urmărite. Cu toate că există un consens general asupra păt îl libertăţii şi prosperităţii ca obiective, nu acelaşi lucru se poate spus despre mijloacele necesare atingerii acestor obiective. Dimpotrivă dacă se poate afirma cu oarecare certitudine că o strategie poliţii I dată poate atinge aceste scopuri, rolul luării deciziilor s-ar diminiie sfârşind prin a dispărea.

Întrucât analiza informaţiilor poate oferi factorului de decr îl indicii privind consecinţele adoptării unei strategii, distincţia teoti tică faptă/valoare nu reuşeşte să identifice rolurile informaţiilor 1 strategiilor. În practică, alegerile factorilor de decizie depind mul mult de părerile acestora legate de consecinţele strategiilor şi unu puţin de selectarea obiectivelor. (într-adevăr, alegerea principalele obiective este considerată atât de evidentă, încât problema e rareoil abordată.) Astfel, se pare că activitatea factorilor de decizie nu cal» atât de clar separată de activitatea experţilor (în acest caz, analişti! de informaţii şi cei ce realizează estimări); deci nu este surprinzătot faptul că relaţia dintre serviciile de informaţii şi factorul politic este» destul de tensionată. Fiecare parte deseori priveşte acţiunile celeilalte părţi ca o încălcare a teritoriului său10.

„Uciderea mesagerului”.

Din perspectiva ofiţerilor de informaţii, disensiunile dintre serviciile de informaţii şi factorul politic par să fie cauzate de cel de-al

doilea Dificultăţile izvorăsc, conform acestora, din tendinţa factorilor tir decizie de a nu acorda atenţie raporturilor de informaţii ce nu sprijin;!

HMitjfiikpolitice pe care doresc să le adopte sau pe care le-au «t'io, ti deja şi faţă de care şi-au luat un angajament. Ofiţerii de nfi Miii, în deseori cred că factorii de decizie sunt interesaţi de ÉMuluicle activităţii de informaţii numai în măsura în care acestea pentru li utilizate pentru a sprijini strategiile politice pe care le-au i „ta, îi din motive complet diferite. Atunci când produsele activităţii J* Informaţii nu sprijină strategiile lor politice, acestea sunt fie înninle, lie se încearcă „ticluirea" lor cu ajutorul presiunilor politice Ht H încât să li se schimbe conţinutul.

Ai castă perspectivă a cristalizat opinia, care tinde să predomine «têi în discuţiile academice, cât şi în cele politice despre serviciile de minimalii, conform căreia cea mai importantă caracteristică a alini ci organizaţii producătoare de informaţii este independenţa util tir factorii de decizie. Numai o agenţie de informaţii înde Mânirnia poate rezista la presiunile politice pe care le-ar putea în h na factorii de decizie pentru a-şi pune de acord preferinţele milmice cu analizele acestora.

În contextul american, s-a oferit astfel cel mai important argument i „unu existenţa unei agenţii de informaţii *centrale* – care să nu fie «ut uită cu niciun departament guvernamental, cum ar fi Depărta irului de Stat sau al Apărării –, cu propriile capacităţi de culegere îi analiză a informaţiilor. O astfel de organizaţie, conform

argumentului „m va fi părtinitoare, lucru ce ar putea distorsiona produsul unui în i viciu de informaţii care face parte din Departamentul de Stat sau ni Apărării şi care este forţat să ţină cont de preferinţele politice ale leanizaţiei-mamă sau de interesele bugetare ale acesteia”.

Această independenţă îi conferă agenţiei de informaţii dreptul de se ghida numai după informaţii, fără să trebuiască să se preocupe li modalitatea în care produsul său va afecta procesul politic. După i am relatează un fost ofiţer superior de informaţii american:

Îmi aduc aminte că, la un moment dat, în calitatea mea de ofiţer de informaţii pe spaţiul Orientului Mijlociu, am fost invitat la Congres pentru a depune mărturie în cazul politicii americane (şi al puşcaşilor marini) din Liban, împreună cu un demnitar de rang înalt din cadrul Departamentului de Stat – numit politic. Pe drum, m-a avertizat că, atunci când voi răspunde la întrebări referitoare la şirul de evenimente din Liban, trebuie să mă limitez ia discuţii despre informaţii foarte actuale şi despre perspectivele pentru următoarele zile. Nu dorea nicio perspectivă cu bătaie lungă. Slavă Domnului că sistemul noului hui permis să ripostez12.

Pe scurt, independenţa ar trebui să ajute la negarea aşa /ieulm sindrom de „ucidere a mesagerului”, tendinţa de a da vina (mm Ht puţin de a-i ignora) pe mesagerii – analişti de informaţii – care, ut veşti supărătoare, analize care nu sprijină strategiile politice lavoiltl

Percepţia comună a acestui sindrom este că

el reflectă o amittihl iraţionalitate din partea factorilor politici; poate cel mai bine»ce ilustrat de fragmentul din *Anioniu şi Cleopatra,* de Shakcspa»i După ce l-a ameninţat pe mesagerul care a informat-o că Antonlu 11 căsătorit cu Octavia, Cleopatra îşi motivează comportamentul N următorul fel:

*Deşi cinstit, nu e niciodată bine să aduci o veste rea. Cu mii de guri*

*Solia bună să o vesteşti; cea proastă* şi *dă singură de ştire când o simţi13*.

O agenţie de informaţii nu ar trebui să se ghideze după ideea 11 nimeni nu ar trebui să fie avertizat în legătură cu evenimente neplăcuta până când acestea nu au loc şi efect. Orice factor de răspundere cât* adoptă o astfel de poziţie ar acţiona într-adevăr într-un mod iraţional

Cu toate acestea, un factor de decizie nu trebuie influenţat da acest motiv iraţional şi să îşi dorească să împiedice o agenţie da informaţii să raporteze veşti nedorite. Într-un stat birocratic modern, niciun demnitar – nici chiar şeful guvernului – nu primeşte în formaţii sau evaluări secrete referitoare la o anumită strategie poliţiei pe care nu o primesc şi alţi demnitari de rang înalt. Unii dintre ceilalţi oficiali s-ar putea să nu fie partizanii politicii şi este de aşteptat ca aceştia să se folosească de informaţiile negative în înecicarea de a contesta sau de a profita de situaţia creată.

Această dificultate este exacerbată numai când informaţiile le sunt împărtăşite nu numai colegilor demnitari şi rivalilor birocratici ai

acestora, ci şi oponenţilor politici (de exemplu, partidul de opoziţie din Congres). Din această perspectivă, nu este deloc iraţional ca factorii de decizie să dorească să se asigure că informaţiile oferit răspunsul „corect”.

Înutfiir, ceea ce este în interesul oricărui factor de decizie nu ** o! însă fie şi în interesul naţiunii. Din punct de vedere naţional, mi Imii să căutăm ceea ce ar conduce la cea mai bună implementare tttn mai bune strategii politice. Din nefericire, aceste două scopuri pa avea cerinţe contradictorii. În general, elaborarea celei mai bune HMii Kii politice necesită ca toate produsele informative relevante să le Ile disponibile tuturor celor implicaţi. Mai mult ca sigur că iulmimaţiile şi analizele secrete vor sprijini argumente atât pro, cât şi… aia oricărei strategii politice propuse; toate aceste argumente ar ilhii cântărite în luarea deciziei finale. Suprimarea accesului la lud urna în sau opinii ori ascunderea acestora faţă de anumiţi iviţii ipanţi la procesul de luarea a deciziilor va înclina balanţa ieih esului şi va reduce posibilitatea obţinerii celui mai bun rezultat.

I îi toate acestea, implementarea pune o problemă diferită; după iie alege o strategie politică, argumentele aduse împotriva acesteia în lui le să fie ignorate în mare măsură. Încercările de a reargumenta iMiiblema de bază a strategiei politice de fiecare dată când trebuie imun o decizie tactică sau de a reorienta strategia după fiecare mini mape nu poate duce decât la o strategie slabă, ambiguă, fluctuantă îi în cele din urmă ineficientă”.

Diseminarea la scară largă a produsului informativ, ce conţine le.n (i care contrazic presupunerile pe care s-a bazat strategia sau care i ellectă în mod negativ asupra progresului acesteia, îi poate părea, li unitarului, ce răspunde de implementarea strategiei, un rău inutil. Iu exprimarea preşedintelui Lyndon Johnson, problema este urmăniarea: „Luarea unor decizii este ca şi când ai mulge o vacă grasă. Vi /i că iese lapte, apeşi şi mai tare şi laptele curge şi, exact atunci aud se umple găleata, vaca o loveşte cu coada şi se varsă totul. Asta l-ai e CIA cu procesul de luare a deciziilor" 15.

Serviciile de informaţii imperiale".

În timp ce analiştii de informaţii deseori cred că ataşamentul unui i.uior de decizie faţă de o strategie îl face să ignore sau să încerce să distorsioneze ori să şteargă informaţii relevante, factorii de decizie pol crede că, deşi informaţiile oferă deseori doar opinii frivole, ar uebui să considere aceste opinii literă de lege şi să ia decizii în onsecinţă. În multe cazuri, nu este clar de ce opinia provenită de la serviciile de informaţii ar trebui considerată mai autoritară hum «fü obiectivă decât opinia altcuiva, inclusiv cea a factorului de din NU De exemplu, deseori o opinie bazată pe informaţii referitoata *k* probleme politice importante nu este bazată pe un nucleu senullill à date concrete (de exemplu, raportul unui agent care activeal h interiorul cabinetului sau al statului-major al adversarului), ti *fß* datele care sunt accesibile şi factorului de decizie (sau unui juritaltM de exemplu). În acest caz, factorul

de decizie poate conaldai justificată decizia de a avea încredere mai degrabă în propria judeţ «Mi decât în cea a unui analist anonim (necunoscut factorului de din / a» «totuşi, criticii acestuia pot afirma că se comportă la fel de iml UIHil şi de ilegal ca şi Cleopatra. Ceea ce poate amplifica tensiunea wfe neputinţa produsului informativ de a clarifica pe ce tip de probi H bazează. (Cu excepţia demnitarilor de rang înalt, este posibil la factorii de decizie să nu afle foarte multe informaţii despre sunar din spatele materialelor scrise pe care le primesc.) Factorul de din,». poate ajunge la concluzia că această lipsă de informaţii referitoare la surse presupune că principalele opinii provenite de la serviciile de informaţii sunt doar de natură speculativă, nefiind bazate pe dala concrete.

În orice caz, probabilitatea ca factorul de decizie să aibă dreptate judecata sa să fie superioară celei a analistului de informaţii – *în* este neapărat redusă. Este adevărat că, cel puţin în Statele Unita, comunitatea factorilor de decizie e uneori caracterizată de un maia procent de demnitari de rang înalt, dând naştere la un anumit grad da amatorism. Este posibil să fie vorba despre faptul că, după cum spun cei din conducerea serviciilor de informaţii, „după câteva luni de activitate [noii analişti de informaţii] devin unii dintre cei mai informaţi oameni din guvern, pe o anumită problematică… Pentru prima dată în viaţa lor, aceştia scriu pentru un public care ştie mat puţin decât ştiu ei” 16.

Totuşi, nu este neapărat aşa şi e posibil ca

factorii de decizie care au expertiza necesară într-un anumit domeniu să desfiinţeze o nota cu informaţii ce reflectă această perspectivă asupra abilităţilor lot Mai mult decât atât, „factorul de decizie poate avea acces direct la informaţii care nu îi sunt accesibile analistului (conversaţii confidenţiale cu demnitari străini, de exemplu) şi, în orice caz, cunoaşte politica Statelor Unite mult mai bine decât analistul – aceasta fiind deseori itoie uusierului" 17. Astfel, în lipsa unei anumite informaţii secrete km «unei metode specializate de analiză, de multe ori opinia ffrtlnului de informaţii nu este îndreptăţită a fi acceptată în detri-fwniiil opiniei altcuiva. După cum a subliniat Charles Fairbanks cu iJvlic în o controversă asupra intenţiilor sovieticilor faţă de Iran în leNin (existenţa unei ameninţări din partea sovieticilor la adresa fonului a constituit o problemă majoră care a afectat politica Statelor 1 Hill1 în ceea ce priveşte această ţară):

Im în ceea ce priveşte mijloacele de analiză utilizate de către comunitatea îi» informaţii, nu există niciun secret în această privinţă: mijlocul este *unaliza*, acelaşi tip de analiză ca şi cea folosită de un demnitar din afara «– unulităţii de informaţii sau cea a unui reporter ori a unui cetăţean în im ercarea de a interpreta fapte asemănătoare. Elaborarea unei Estimări de Informaţii Naţionale Speciale (SNIE) pe o astfel de problematică… «.în de fapt acelaşi exerciţiu ca şi cel realizat, în sensul bun sau prost, de uliul dintre membri echipei [Consiliului Naţional de Securitate] atunci când.i hotărât să vândă arme

Iranului. Este un exerciţiu de raponament politic18.

Numai atunci când rezultatul unui astfel de proces de raţionare tu uneşte eticheta de „informaţie” (şi o ştampilă cu caracterul documentului) se poate pretinde că este vorba de „un nucleu concret de lupte care transcende argumentele politice dubioase sau interesate de altor agenţii şi care va servi ca test neutru de evaluare a acestora”, 9.

Aceeaşi situaţie poate apărea atunci când există „fapte concrete” disponibile analistului de informaţii, pentru că sunt rare situaţiile în me aceste fapte sunt înţelese de la sine. Acestea trebuie interpretate iun un anumit context, care este furnizat, în primul rând, de către maust. Cu toate acestea, contextul se bazează pe raţionamentul speculativ în privinţa căruia este posibil ca analistul să nu aibă un iivantaj special faţă de factorul de decizie. După cum sublinia Graham I uller, un fost ofiţer de informaţii pe spaţiul Orientului Mijlociu.

Pe măsură ce informaţiile devin mai generale, de natură strategică, creşte şi sensibilitatea interpretării acestora... [De exemplu, întrebări de genul] cât vor rămâne la putere tiranii geriatrici de la Beijing? Dacă Saddam este înlăturat de la putere, se va scinda Irakul? Va reuşi Europa să menţină NATO?... [reprezintă] materiale pentru informaţii strategice. Este important ca analiştii să aibă datele, dar, până la urmă, e nevoie de raţiune pentru a încerca să dea răspunsuri[,]... [iar astfel de raţionamente vor face apel la percepţia

generală a individului despre „cum *im* ţionează lumea”... o perspectivă coerentă asupra politicii internalliatali Acest gen de înţelegere este ideologică prin natura sa... pentru că llttËÉ o ordine... într-un amalgam foarte difuz de date şi evenimente... Nfi-e altceva nu poate învinge acest modern surplus de informaţii. Mari lipsa unei astfel de construcţii este echivalentă cu apariţia unei Itttiuvfitf extrem de superficiale a problemelor umane20.

Aceste argumente sunt contrare fluxului de opinii actuale de \ \ acest subiect, care evidenţiază importanţa menţinerii independenţii serviciilor de informaţii faţă de politic şi a forţării politicului să la M în considerare. Acordul dintre o strategie politică şi informalllli secrete este deseori considerat o apreciere a raţionalităţii acenif»le însă se pierde orice sens al solidităţii informaţiilor însele – se buze«n! pe un fapt incontestabil sau pe o speculaţie destul de contestabili f

Acest punct de vedere poate fi luat în seamă şi în ceea ce privat U circumstanţele apariţiei articolului lui Fairbanks din care am citat anterior. Informaţii referitoare la elaborarea unei SNIE, la care tot e referire – conform căreia posibilitatea ca sovieticii să invadeze Iranul era relativ mică –, au fost transmise presei pe cale neoficială, evident pentru a critica „vânzarea de arme către Iran în secret, pe cart preşedintele Reagan a ordonat-o în ianuarie 1986 pentru a sprijin) Iranul împotriva «intervenţiilor din partea Uniunii Sovietice»”, la articolul în care a apărut această scurgere de informaţii, se susţină a că „analiza pare să pună

sub semnul întrebării o analiză primaţi raţională a Casei Albe" 21. Cu alte cuvinte, raţionamentul pe baia informaţiilor a fost utilizat ca piatră de temelie pentru o strategia politică, în ciuda „concreteţii" dovezilor pe care s-a bazat.

Acest tip de controversă are loc din cauza importanţei acordala „independenţei" serviciilor secrete din sistemul american. Prin comparaţie, sistemele de informaţii ale altor ţări (cum ar fi Marea Britanie) sunt mai puţin preocupate de protejarea „purităţii" ratio namentelor bazate pe informaţii şi mai interesate să se asigure cil expertiza proprie a factorilor de decizie poate contribui la procesul estimativ. După cum observă Loch Johnson:

Produsul final american este o estimare *informativă*, pe când cel britanii e o evaluare mai generală care presupune o combinaţie între raţionamentul politic *şi* cel al ofiţerilor de informaţii... De fapt, cultura britanici im, mulează combinarea [informaţiilor secrete cu strategia politică], în ţintuita că deciziile politice cele mai bune rezultă mai degrabă din i... hui de experienţă dintre specialiştii în afaceri internaţionale ai

Jim".

Mwprindenţa serviciilor secrete linul potenţialele surse de fricţiune din relaţia dintre serviciile Hilm îi taţii şi factorul politic, problema privind gradul de independenţă l»f viciilor secrete faţă de factorul politic este foarte complicată. În Nitul structurilor militare, de exemplu, ofiţerul de informaţii de le " superior face parte din echipa comandantului în aceeaşi măsură îi un i la fel de

subordonat) ca şi orice alt locţiitor; nici nu se pune *îi* iilrnia independenţei. Într-adevăr, nici măcar adevăratul sens al –» Minţii ca o agenţie de informaţii să fie „independentă” nu este Ui în principiu, nimeni nu ar susţine independenţa unui serviciu în informaţii faţă de şeful guvernului. Cu toate acestea, după cum itoin n şi discuţiile de mai sus, se doreşte deseori ca informaţiile să în utilizate drept criteriu neutru de arbitraj în cadrul disputelor, mitiu e – nu numai dintre oficialii din guvern, ci şi dintre oficialii *Nu* guvern şi criticii lor legislativi şi extraguvernamentali. Aceasta implică independenţa faţă de toate autorităţile guvernamentale şi o îi iponsabilitate directă, corespunzătoare faţă de alt grup, un corp li gistativ (ca reprezentant al opiniei publice) sau chiar opinia publică.

După cum am discutat anterior, principalul argument în favoarea „lependenţei derivă din sindromul „uciderii mesagerului”: serviciile li informaţii trebuie să fie independente dacă analiştii trebuie să fie ipabili să spună adevărul aşa cum îl percep ei. În acest context, independenţa înseamnă capacitatea de a proteja analiştii individuali li presiunile sau ameninţările care i-ar putea determina să facă. «meluziile trase de ei mai acceptabile pentru beneficiarul produsului. Iun o oarecare măsură, acest gen de independenţă poate fi realizată în crearea unei agenţii *centrale* de informaţii, care se subordonează fiului guvernului, dar nu şi beneficiarilor importanţi ai unormaţiilor, cum ar fi departamentul sau ministerul Afacerilor l (terne

sau al apărării naţionale. Cu toate acestea, înşişi şefii guvernelor sunt beneficiari ai informaţiilor, deşi poate au investit o mare parte din propria imagine într-o strategie politică. În acest caz, problema reapare la un nivel superior. Până la urmă, a (At tlmp serviciul de informaţii face parte din guvern, singura măittffp siguranţă este verticalitatea directorilor serviciilor de informat disponibilitatea şi abilitatea acestora de a proteja analiştii de pitite exterioare.

Independenţa este deosebit de importantă atunci când e»to itJHUŢ să fie abandonate strategiile politice care nu dau rezultate sau i aia devenit învechite ori contraproductive ca urmare a schimb Aill»a cumstanţelor în care erau aplicate. În acest scop, unele mec unim* trebuie să prezinte asigurări că toate informaţiile relevante, pnjititt şi negative, sunt disponibile pentru implementarea strategiei pul în După cum sugerează citatul din Johnson, factorii de decizie ti? iMt să-şi canalizeze mare parte din energie implementării strategitl* politice, cu oarecare consecvenţă, în ciuda permanentelor conttteU îndoieli, atacuri politice – nu neapărat motivate de convins” sinceră în ceea ce priveşte superioritatea altei strategii politice 1 aşa mai departe. În aceste condiţii, este deosebit de dificil prun astfel de oficiali să schimbe macazul şi să elaboreze o reviwtm lipsită de prejudecăţi a strategiei politice.

În această situaţie, serviciile secrete au o poziţie de advenu, întrucât evidenţierea domeniilor în care strategia politică nu 41 rezultate sau a devenit inadecvată devine cea mai

importantă lump, a lor. Cu alte cuvinte, acestea trebuie să contracareze presiuim politică exercitată asupra birocraţilor pentru a-i determina să fie bunt coechipieri strategiile politice actuale. De aceea, serviciul di informaţii care prezintă o informare ce sugerează că strategia pollltol este învechită sau că obiectivul acesteia este greşit trebuie să alht destulă independenţă pentru a rezista la presiunile generate de 11 astfel de situaţie.

În trecut, o astfel de situaţie, care a atras atenţia opiniei publici, s-a referit la rolul comunităţii de informaţii în verificarea respectării acordurilor privind controlul armelor. Acuzaţia că una dintre părţir semnatare a încălcat acordul privind controlul armelor ar pune sub semnul întrebării decizia încheierii acestui acord de la bun început sau, oricum, decizia continuării aderării la el. Dorinţa de a menţine acordul (sau de a păstra ori a ameliora în general relaţiile cu partea respectivă) a oferit un motiv puternic de a ignora sau a ascunde dovezile incomode. În orice caz, dificultatea întâmpinată în t»te n»fii tic a forţa partea respectivă să respecte acordul sau de a fi»iuiiule orice măsură care vizează încălcarea acordului a fost şi é»o un factor determinant pentru a nega existenţa acesteia.

Iu plus, un serviciu de informaţii trebuie să fie suficient de U»I«uilent pentru a lua iniţiativa de a cerceta probleme sau zone Imun fără să fie nevoie să i se ordone acest lucru de către (MIM iuii, iiea de factori politici. Un serviciu de informaţii ar trebui să 4Ht»/e orizontul pentru a

depista potenţiale probleme din zonele H««ni, mag atenţia factorilor de decizie. Această funcţie de avertizare rlie-n inevitabil înaintarea către factorii de decizie a unor informaţii

* iiir aceştia nu le-au cerut şi pe care nu le doresc în mod special, i Mim că nu le cunosc valoarea.

Dai independenţa prezintă şi dezavantaje. Poate cel mai mare hulii acestea este riscul ca în cursul procesului de adoptare a uior politice munca de culegere a informaţiilor să devină sau ni, percepută ca irelevantă. Această situaţie poate apărea pentru că hăul de informaţii nu ştie ce probleme sunt considerate a fi mai iuNiiiante de factorii de decizie sau ce opţiuni pot fi luate în i. Muvrare pentru rezolvarea lor.

Această problemă poate fi cauzată nu doar de simpla distanţă «iMiu/acţională sau fizică faţă de factorii de decizie. Analiştii de ini… am deseori refuză să coopereze în ceea ce priveşte implementarea

». urgiilor politice pe care nu le susţin. Fostul director ai CIA, M«ilmtl Gates, a oferit un exemplu care să ilustreze această problemă:

Munci când secretarul de stat Alexander Haig a afirmat că sovieticii se illa în spatele terorismului internaţional, iniţial, analiştii de informaţii im şi-au propus să abordeze problema din toate punctele de vedere, ci mai degrabă să dovedească faptul că secretarul nu avea dreptate – pur şi simplu să demonstreze că sovieticii nu orchestrează întregul terorism internaţional. Dar prin această abordare ei înşişi au mers prea

departe şi nu au reuşit iniţial să descrie vasta şi bine documentata susţinere indirectă.1 grupărilor teroriste şi a sponsorilor acestora de către sovietici23.

cu alte cuvinte, o strategie de abordare a problemei terorismului micrnaţional ce ar fi obligat URSS să îşi reducă sprijinul (direct sau m. li rect) acordat grupărilor teroriste a fost zădărnicită de faptul că maliştii serviciilor secrete nu au fost dispuşi să coopereze, considerând.10 astfel de implicare a Uniunii Sovietice nu constituia decât o parte nesemnificativă a problemei terorismului. Poate că în * *§ idee era fundamentată, dar nu înseamnă că strategia respectivi în incorectă; este posibil, de exemplu, ca politica Statelor Unit* Mi în fi fost în măsură să abordeze principalele cauze psiholog» § sociologice sau chiar politice ale terorismului sau rezolvffe acestor probleme să fi intrat în conflict cu alte obiective de pulitfcé externă.

Dacă serviciile de informaţii se concentrează prea mult «r «acest lucru este necesar) asupra adoptării unei poziţii adventt (ţfe exemplu, în cazul implicării în revizuirea strategiilor adopt, it, devine tot mai dificil ca acestea să sprijine implementarea efectivi strategiilor. Asumarea unui rol de sprijin presupune ca serviciile th informaţii să-şi concentreze eforturile asupra identificării şi anall/câte informaţiilor relevante pentru implementarea strategiei. În exemplul de mai sus, aceasta ar fi însemnat descoperirea mecanismelor ptiu care o grupare teroristă internaţională a primit asistenţă financiari t logistică de la

susţinătorii ei. Pentru a sprijini implementarea mm tegiei, un serviciu de informaţii ar trebui să nu insiste asupra conceptţW sale – potrivit căreia sprijinul acordat de un stat nu constitui! cauză principală a terorismului internaţional – cu privire la motivelf pentru care strategia este eronată.

Serviciile secrete şi „era informaţională".

Progresul rapid al tehnologiei în domeniul telecomunicaţiilor şi al prelucrării datelor – principalele tehnologii specifice aşa-numitei „ere informaţionale" – a provocat schimbări ample în modul în care organizaţiile utilizează informaţiile24. Un factor deosebit de important a fost explozia informaţiilor din surse deschise. Pe lângă utilizarea pe scară largă a internetului, prăbuşirea comunismului sovietic a fost poate cea mai importantă cauză care a facilitat accesul la informaţiile din surse deschise: de la Vladivostok la fluviul Elba (care marchea/fi frontiera dintre fosta Germanie de Vest şi cea de Est) dispăruse un întreg aparat menit să păstreze secretul chiar şi asupra celor mai banale evenimente.

În general, procesul cunoscut sub denumirea „globalizare" a inteusi ficat circulaţia transfrontalieră a informaţiilor şi a creat multe în tir noi de informaţii. Globalizarea este un concept greu de – l. hun; probabil cea mai importantă manifestare a sa este intentait mea comerţului internaţional şi a diviziunii muncii, care s-a Huit simţită în majoritatea statelor lumii. Acest lucru a dus la Muierea numărului de deplasări şi la răspândirea mijloacelor de Informare din ţările dezvoltate în întreaga lume (de exemplu, difuim.1

CNN şi a altor canale de ştiri în hotelurile din diferite regiuni

Ilumii).

Chiar înainte de începerea erei informaţionale, factorii de decizie aveau acces la multe informaţii provenite din alte surse decât cele n adiţionale. Schimbările apărute în mediul politic internaţional şi ele determinate de „revoluţia informaţională" sugerează că în viitor vini li disponibile şi mai multe informaţii provenite din afara serviciilor în i icte.

Deşi existenţa şi accesibilitatea tot mai mare ale surselor de minunaţii din afara canalelor tradiţionale prezintă avantaje importante (miiuu factorii de decizie, ele creează şi o serie de probleme, legate de:

localizarea acestor surse; evaluarea credibilităţii lor; analizarea informaţiilor pe care le furnizează şi coroborarea acestora cu datele obţinute de la serviciile de informaţii; păstrarea confidenţialităţii cu privire la aspectele de interes pentru factorii de decizie.

Deşi aceste probleme nu sunt noi, se pune întrebarea dacă schimbările aduse de era informaţională sunt de o asemenea amploare încât să impună abordarea lor într-o manieră mai sistematică decât până acum. Factorii de decizie au nevoie de „specialişti în informaţii" pentru a-i ajuta să selecteze anumite informaţii din multitudinea celor existente în era informaţională? în prezent, această funcţie este îndeplinită în trei modalităţi:

de către factorii de decizie; de către

personalul subordonat acestora; de către analiştii de informaţii.

Fiecare dintre aceste modalităţi prezintă anumite avantaj» t dezavantaje. Desigur, factorii de decizie sunt responsabili pinme acţiunile lor şi, prin urmare, trebuie să se asigure că au primii l cu înţeles corect informaţiile relevante. Astfel, cel puţin o palte i procesului de analiză le aparţine. De asemenea, aşa cum ani…

ţionat deja, ei pot avea acces la surse de informaţii indisponlhtit pentru alţii: comunicaţii la nivel înalt cu alte guverne, precum îi intenţiile şi planurile unor oficiali din cadrul propriului guvern ţi ni» unor factori neguvernamentali (cum ar fi anumiţi membri impoiiauu ai comunităţii de afaceri, specialişti cu experienţă etc.). În plus, unii factori de decizie au o experienţă mai vastă în domeniul vizat din el analiştii de informaţii sau personalul din subordine.

De asemenea, factorii de decizie au prea multe de făcut pentru se ocupa şi de culegerea şi analizarea informaţiilor, dincolo de faptul că citesc ziarele, telegramele cu caracter secret (care nu pot fi lăsiM* în seama subordonaţilor) şi materialele selectate de personalul lui în mod inevitabil, cele mai multe informaţii le vor fi transmise nuli formă de extrase sau evaluări deja întocmite, prezentate verbal sau la scris.

Spre deosebire de şefii lor, subordonaţii pot avea timpul neccMU pentru a culege şi a analiza multe dintre informaţiile necesare. AvAiul în vedere că aceştia sunt implicaţi şi în procesul decizional, ei trebuie să ştie ce aspecte sunt

relevante, care sunt obiectivele urmărite şi aţa mai departe. Cu excepţia chestiunilor secrete, ei au cunoştinţă de interacţiunile cu alte guverne sau alţi membri ai propriului guvern în general, ei se bucură de încrederea şefilor lor; totuşi, pot exista cazuri în care superiorii doresc să analizeze anumite aspecte fără ca subordonaţii lor să cunoască acest lucru.

Cu toate acestea, este posibil ca membrii personalului să se concentreze mai mult asupra elaborării strategiilor decât asupra culegerii şi analizării informaţiilor. În consecinţă, ei ar putea să nu acumuleze experienţa necesară în domeniul informaţiilor. În orice caz, aceste responsabilităţi pe linie de informaţii vor avea o pondere mai redusă decât cele referitoare la elaborarea strategiilor; angajaţii nu au în general timpul necesar pentru a-şi dezvolta nivelul de cunoştinţe dincolo de „capitalul intelectual" pe care îl deţineau deja la numirea în funcţie. De asemenea, ei nu au acces şi nici experienţa necesară în ceea ce priveşte sursele şi metodele specifice activităţii *e* mI«amaţii; astfel, este posibil ca ei să nu poată corobora informaţiile inamic de la serviciile secrete cu alte categorii de date. Totodată, ei pa îl supuşi unor presiuni din partea superiorilor, care doresc să se iifc Mâncă analizele realizate corespund opţiunilor lor strategice sau *fa* 1/iilor deja adoptate.

Dr asemenea, analiştii de informaţii se concentrează exclusiv MMjaa sarcinilor ce le revin pe linie de informaţii şi nu sunt direct

* în msabili pentru alegerea anumitor

strategii. Cariera lor profesională». desfăşoară numai în sfera informaţiilor, deşi adesea analiştii loiuric să îşi asume atribuţii manageriale pentru a putea evolua în flau profesional. Aceştia nefiind implicaţi în procesul decizional, im linilor de decizie le-ar putea fi mai uşor să le pună întrebări ii-Urtic de opţiunile strategice, care sunt prea controversate pentru a fi, li /bătute într-un cadru politic mai larg. Analiştii au acces şi sunt iiiuliarizaţi cu sursele şi metodele specifice activităţii de informaţii II Mint astfel în măsură să coroboreze datele primite pe aceste canale h alte informaţii. În cele din urmă, ei sunt (sau cel puţin ar trebui he) pregătiţi să evalueze dacă anumite informaţii aparent veridice mul, de fapt, rezultatul eforturilor de deziirformare ale adversarilor.

lotuşi, analiştii de informaţii se confruntă şi cu anumite dezavantaje. Necunoaşterea opţiunilor strategice ale propriului guvern poate face i, i rezultatul activităţii lor să fie mai puţin util decât ar fi în alte i undiţii, deoarece îi reduce relevanţa şi oportunitatea şi, totodată, poate conduce la o subestimare a măsurii în care acţiunile altora aniicipează sau sunt o reacţie la propriile acţiuni. În special, „tabuul" legat de analiza propriilor capacităţi sau strategii poate face dificilă i inturarea unei imagini clare şi utile a „echilibrului de forţe" existent în raport cu partea adversă. În plus, analiştii de informaţii pot avea lendinţa de a ignora sursele din afara canalelor secrete obişnuite, deoarece credibilitatea lor ar putea fi mai greu de stabilit, iar furnizorii de informaţii din afara aparatului guvernamental (cum ar fi oamenii

de ştiinţă sau afaceriştii) ar putea fi mai puţin dispuşi să coopereze în un serviciu de informaţii decât cu o agenţie guvernamentală.

Probabil că nu va exista o soluţie unică aplicabilă în toate cazurile, lotuşi, ar putea fi util ca factorii de decizie să ia în considerare procedurile aplicate în acest domeniu de aparatul militar. De regulă, un comandant are în subordinea sa un ofiţer de informaţii („G-2", în limbajul armatei americane). Acest ofiţer este specializat în probleme legate de informaţii, dar lucrează pentru comandantul său, l tty pentru un serviciu de informaţii. El are sarcina de a obţine, a tumll* şi a interpreta *toate* informaţiile relevante, indiferent dacă provin de surse secrete, din alte surse guvernamentale sau din surse dewhlH în plus, datorită pregătirii sale şi relaţiilor pe care le are cu să v cu HU secrete, el poate fi mai mult decât un destinatar pasiv al informaţiili t el poate să caute la nivelul serviciilor secrete datele necesare COfNl dantului său şi să îi susţină priorităţile cu privire la culegeroi ţ) diseminarea informaţiilor.

Activitatea de informaţii şi democraţia

Democraţia şi confidenţialitatea informaţiilor

Confidenţialitatea, aşa cum am remarcat deja, ridică o potenţiali problemă în ceea ce priveşte exercitarea controlului asupra serviciilnt de informaţii de către organismele de supraveghere din afara comunităţil de informaţii. Nevoia legitimă de a limita cunoaşterea unor detalii ale operaţiunilor desfăşurate la un cerc cât mai restrâns poate ni ducă la camuflarea unor

acţiuni neautorizate, împiedicând astfel autorităţile din afara comunităţii de informaţii să ia cunoştinţă de respectivele operaţiuni.

Într-o societate democratică, confidenţialitatea ridică însă şi o altă problemă: posibilitatea de a pune sub semnul întrebării legitimitate» politică a unui serviciu de informaţii, spre deosebire de controlul propriu-zis. Dacă democraţia reprezintă nu numai conducerea în interesul poporului, ci şi exercitarea ei de către popor, nu este de mirare că instituţiile pentru care confidenţialitatea este un aspect extrem de important pot deveni foarte uşor ţinte ale neîncrederii populaţiei. Această suspiciune nu se limitează doar la serviciile secrete. Promisiunea făcută de preşedintele Woodrow Wilson că problemele internaţionale ale perioadei de după Primul Război Mon dial aveau să fie soluţionate „prin înţelegeri publice, adoptate în urma unei dezbateri publice” reflecta suspiciunea oamenilor de rând faţă de diplomaţia antebelică şi faţă de caracterul secret în general.

t»muolul legislativ şi al societăţii civile

!» purismul privind confidenţialitatea existentă la nivel guvernamental Mii probabil un fenomen endemic în societăţile democratice şi a mmhliis în Statele Unite şi, într-o măsură mai mică, în alte lări»Ihih h iatice la necesitatea exercitării controlului asupra serviciilor»i. Informaţii de către anumite organisme guvernamentale care se t»me urii de independenţă în raport cu şeful statului. În Statele Unite,”, i stabilit la mijlocul anilor ’70 un sistem

de control exercitat de an r Congres prin intermediul a două comisii create în acest scop H omisia Specială Permanentă a Camerei Reprezentanţilor pentru iivitatea serviciilor de informaţii şi Comisia Specială a Senatului l» «uliu activitatea serviciilor de informaţii).

Piatra de temelie a acestui sistem de control o constituie obligaţia I«pala a preşedintelui de a „informa permanent şi complet aceste misii cu privire la activităţile de informaţii" desfăşurate de diverse itiucturi guvernamentale25. Dreptul celor două comisii de a fi informate «*v* deosebit de important, ţinând cont şi de prerogativele Congresului. u privire la alocarea unor fonduri. Potrivit lui Robert Gates, rezultatul ale că, în anumite situaţii:

procesul de control a conferit Congresului – în special celor două comisii pentru controlul activităţii serviciilor de informaţii – o cunoaştere mult mai completă şi o influenţă mult mai mare decât a oricărei structuri din cadrul executivului asupra modului în care CIA şi alte servicii de informaţii îşi cheltuiesc bugetul, de la cheltuieli de ordinul miliardelor de dolari la achiziţii de ordinul miilor… în prezent, Congresul poate avea mai multă influenţă asupra priorităţilor CIA şi asupra modului de alocare a resurselor decât executivul26.

Sistemul de control exercitat de Congres poate fi privit ca un i omoromis între necesitatea menţinerii confidenţialităţii şi cea de a.pori influenţa opiniei publice asupra serviciilor de informaţii, astfel încât să se asigure că serviciile

secrete nu utilizează mijloace şi nu în măresc obiective pe care opinia publică le-ar dezaproba. Controlul exercitat de Congres permite comisiilor pe probleme de informaţii să fie substitute ale dezbaterii mai ample (în cadrul executivului, al (ongresului şi în rândul populaţiei) care ar însoţi adoptarea altor strategii sau iniţiative guvernamentale.

Ambiguitatea creată prin utilizarea comisiilor ca substitui) opiniei publice este sesizată mai ales atunci când este vorba îţi acţiunile secrete, problemă care a condus de fapt la instituirii actualului sistem de control exercitat de către Congres. Baza legali pentru rolul comisiilor este cerinţa ca ele să fie notificate de fiocatf dată când preşedintele ordonă o acţiune secretă. Deşi cerinţa mtficării nu implică, în principiu, prerogative de veto, obiecţiile putertttoe ale membrilor comisiilor pot duce la revizuirea sau chiar la anulaţii unei propuneri de acţiune secretă atunci când consecinţele poliţiei ale unei astfel de acţiuni par să fie mai importante decât rezult, de I«estimate27. Astfel, unul dintre scopurile notificării prealabile poali fi descris ca fiind o testare a propunerii în faţa unui segment (relativ restrâns) al opiniei politice, reprezentat de persoane independente tla preşedinte, pentru a stabili dacă propunerea corespunde sau tat principiilor şi valorilor fundamentale.

Lăsând la o parte această funcţie de substitut al dezbaterilnt publice, transmiterea informaţiilor referitoare la acţiuni secrete cai 11 membrii Congresului dă posibilitatea punerii în practică a

preru gativelor Congresului în materie de alocare a fondurilor. AccMti prerogative pot să fie exercitate de către comisiile pe probleme da informaţii sau să implice o dezbatere la nivelul Senatului şi al Camerei Reprezentanţilor; aşa s-a întâmplat în cazul „amen damentelor Boland" prin care se limita sau se interzicea sprijinirea mişcării de rezistenţă din Nicaragua în anii ’8028.

Principalul argument în favoarea exercitării controlului de către Congres asupra acţiunilor secrete este că întruneşte avantajele controlului democratic, pe de o parte, şi cele ale păstrării confidenţialităţii, pe de altă parte. Analiza în cadrul comisiilor reprezintă un substitut al unei dezbateri publice efective şi al procesului democratic uzual de luare a deciziilor – acestea fiind, bineînţeles, incompatibile cu păstrarea confidenţialităţii.

Valabilitatea acestui argument a fost însă contestată deopotrivă din perspectivă practică şi teoretică. Practic, problema este dacă nu cumva controlul exercitat de către Congres conduce inevitabil la divulgarea informaţiilor, indiferent de prevederile regulamentelor de fapt, există puţine date certe privind sursa numeroaselor scurgeri de informaţii legate de acţiunile secrete, iar investigarea anumitoi cazuri de acest fel nu dă aproape niciodată rezultate. Având în vedere

Imputtanţa pe care o acordă jurnaliştii păstrării confidenţialităţii UMirlore acest lucru nu este deloc surprinzător29.

În orice caz, nu există nicio îndoială că sistemul de control al I»mwleşului conduce la

creşterea numărului persoanelor care au h t’s la informaţiile privind acţiunile secrete. În general, riscul unei

* în f ci i se informaţii depinde de numărul de persoane care au acces M Informaţii. De asemenea, congresmenii şi personalul din subordinea Im sunt, de regulă, mai puţin obişnuiţi să lucreze cu informaţii i l.uulicate şi îşi desfăşoară activitatea într-un mediu cu un caracter politic mai pronunţat decât cel specific unui ofiţer de informaţii, i «i uita de a informa Congresul presupune probabil implicarea unor (h isoane din cadrul executivului, având în vedere că trebuie să fie MIM în temă şi o serie de persoane care se ocupă de relaţiile ailnunistraţiei cu Congresul. În majoritatea cazurilor, destul de mulţi miajaţi din cadrul executivului au acces la informaţii, astfel încât, lupa toate probabilităţile, creşterea numărului celor care intră în i\esia informaţiilor ca urmare a controlului exercitat de Congres nu iirle semnificativ riscul unor scurgeri de informaţii; în cazuri tpreiate, când accesul este limitat la un număr restrâns de persoane lin cadrul executivului, odată cu creşterea numărului celor care află dalele respective, se amplifică şi riscul producerii unor scurgeri de ml oimaţii.

Deşi, în mare parte, dezbaterea publică declanşată pe marginea ontrolului exercitat de Congres odată cu instituirea acestui sistem privea scurgerile de informaţii, problema de natură teoretică legată le acest sistem de control asupra acţiunilor secrete priveşte necesitatea li eficienţa adoptării de către Congres a unor proceduri

secrete ca în nvitate de rutină.

Astfel, un fost oficial al Uniunii pentru Libertăţile Civile din America, Morton Halperin, a depus mărturie în faţa Comisiei Church, ducând argumente împotriva conceptului:

I Aplicarea unor forme mai bune de control] nu reuşeşte să elimine dezavantajele inerente deţinerii unor atribuţii în ceea ce priveşte derularea acţiunilor secrete. Singura armă pe care o au la dispoziţie opozanţii unei politici prezidenţiale, din interiorul sau din afara executivului, este dezbaterea publică. Dacă o strategie poate fi dezbătută public, atunci Congresul poate fi convins să exercite presiuni asupra preşedintelui, iar presiunile din partea opiniei publice pot determina o schimbau în strategie. Dar, dacă se acceptă legitimitatea ideii de confidentul Matt atunci măsurile de control asupra operaţiunilor secrete pot fi ignor e în uşurinţă30.

Deşi această apreciere s-a dovedit a nu lua în considerare rezullnlet pe care le pot obţine comisiile Congresului prin negocieri tili caracter public cu executivul (existând permanent ameninţarea dai văluirii informaţiilor), ea conţine un sâmbure de adevăr: în ui/ni unor divergenţe majore de opinii, cum ar fi sprijinul „secret” acordat mişcării de rezistenţă din Nicaragua în anii ’80, s-a renunţat la păstrarea confidenţialităţii şi problemele au fost dezbătute de Congiin în mod public.

Astfel, ideea controlului exercitat de Congres în condiţiile păsârAMI confidenţialităţii include o

contradicţie în termeni: se urmărela obţinerea beneficiilor aferente deliberării problemelor legate da informaţii în cadrul legislativului, dar se exclude de la bun început principala metodă utilizată într-o astfel de deliberare – dezbaterea amplă, cu caracter public.

Aceste aspecte privind păstrarea confidenţialităţii şi controlul activităţii de informaţii se confundă adesea cu o altă chestiune, total diferită: în ce măsură faptul că un stat este democratic influenţea/l politica externă pe care ar trebui să o adopte? Acest lucru cala valabil, în special, cu privire la acţiunile secrete, aspect al activităţii de informaţii care, în Statele Unite, a atras cele mai multe critici pa motiv că ar fi antidemocratice. Totuşi, majoritatea criticilor la adrcua CIA privind acţiunile secrete desfăşurate ar fi trebuit să fie îndreptata mai degrabă împotriva strategiilor de politică externă care prevedeau astfel de acţiuni.

În Statele Unite, principala nemulţumire legată de acţiunile secrete din anii ’70 şi 80 viza faptul că reprezentau un amestec în treburile interne ale altor ţări. Caracterul secret sau public al intervenţiei respective era, se pare, un aspect secundar. S-a argumentat uneori el o asemenea acţiune este nedemocratică, în sensul că se realizează în secret tocmai pentru că ar fi întâmpinat o opoziţie puternică din partea opiniei publice dacă ar fi fost cunoscută. Situaţia nu este însă atât de clară precum pretind cei care invocă aceste argumente. De exemplu, diferitele acţiuni secrete îndreptate împotriva lui Fidel lilio, inclusiv

tentativele de asasinat, s-ar fi putut bucura de sprijin ppulat la momentul la care au avut loc. Atunci când Comisia Church I uhlectat că astfel de acţiuni nu beneficiau de susţinerea opiniei Utllcc americane, aceasta a analizat acţiunile secrete întreprinse în Mh în de CIA nu prin raportare la opinia publică de la sfârşitul tulim 50 şi începutul anilor ’60 (atunci când au avut loc tentativele), îl în opinia publică de după Războiul din Vietnam, de la mijlocul «mloi 7031. În jurul anilor ’90, opinia publică a înregistrat o nouă liimbare, acceptând cu uşurinţă intervenţia americanilor în trebuhlf interne ale statelor Haiti şi Iugoslavia (cu privire la Kosovo).

I ar la mijlocul anilor ’70, când au fost înfiinţate comisiile de in nu ol pe probleme de informaţii din cadrul Congresului Statelor l mic, şi alte ţări democratice au avut în vedere constituirea unor iMtanisme independente de control al activităţii de informaţii. De Întâmplu, în 1984, Parlamentul canadian a înfiinţat Comisia de un! i/;1 a activităţilor de informaţii privind securitatea (SIRC), pentru ne uitarea controlului asupra aparatului intern de informaţii, care a inul separat de Serviciul Regal Canadian al Poliţiei Călare şi a fost ihiiislormat într-o agenţie civilă, Serviciul Canadian de Informaţii l»iivind Securitatea.

Spre deosebire de comisiile de control din SUA, SIRC nu este o

«misie a parlamentului, ci e alcătuită din consilieri numiţi de i»şi nu ministru în urma unor consultări cu liderii partidelor de opoziţie. «i i

msiliul privat este un grup ai cărui membri, de obicei foşti membri ni (abinetului, au fost recunoscuţi oficial de către guvernul canadian în calitate de consilieri.) SIRC prezintă un raport anual în faţa l cu lamentului, dar nu are prerogative legislative sau în materie de lui get. Diferenţa dintre mecanismele de control din Canada şi cele Im SUA reflectă diferenţele dintre cele două sisteme politice; în.i.icmul american, principalele divergenţe apar între executiv şi li y.islativ, ceea ce nu se întâmplă în sistemul parlamentar canadian, care caracterizează printr-o puternică disciplină de partid. (în astfel de i.lerne, prim-ministrul este liderul partidului sau al coaliţiei de i mii de ce deţine majoritatea locurilor în parlament şi este el însuşi membru al parlamentului.) în Canada, independenţa necesară faţă le i»uterea executivă se obţine cu sprijinul unor eminenţi oameni de stat32.

Alte ţări, printre care Marea Britanie, Australia33, Noua Zeelandă i (ïermania, au creat comisii parlamentare cu atribuţii de control, deşi aceste comisii se deosebesc în mai multe privinţe de modi american34. Principala diferenţă, aşa cum am arătat mai sus, oul» t respectivele sisteme parlamentare nu permit independenţa legulatiti inerentă sistemului prezidenţial al Statelor Unite, caracterizat pttn separarea dintre puterea executivă şi cea legislativă. Astfel, în Mat* Britanie, membrii Comisiei pentru Informaţii şi Securitate mi-a „numiţi de către prim-ministru, în urma consultărilor cu Udatul opoziţiei" („opoziţia" fiind partidul sau coaliţia minoritar* un parlament)

35. De asemenea, comisia îl informează pe prim-minuthi, care, înainte de a prezenta informarea în faţa parlamentului, „poala l excludă materialele care consideră că ar aduce atingere îndepliniţii atribuţiilor agenţiilor, după ce se consultă cu membrii Comisiei – Mi în plus, sfera de responsabilitate a acestor comisii este diferit! Astfel, conform legii privind înfiinţarea sa, competenţele de investigaţii ale Comisiei Parlamentare Comune pentru Controlul Agenţiei Australiern* de Informaţii şi Securitate (ASIO) nu cuprind şi „aspecte ce ţiu da obţinerea sau comunicarea de către ASIO a informaţiilor externa" sau „aspectele activităţii ASIO care nu afectează cetăţenii australieni sau persoanele cu rezidenţă permanentă" 37.

Democraţia, activitatea de contrainformaţii şi informaţiile interne

De fapt, contrainformaţiile, nu acţiunile secrete reprezintă elementul activităţii de informaţii ce este cel mai puternic afectat de natuta democratică a regimului pe care îl deserveşte. Cele mai multe dintre dificultăţile ce apar în relaţia dintre democraţie şi activitatea de informaţii privesc contrainformaţiile. Aceste dificultăţi privesc, în special, stabilirea situaţiilor în care o agenţie guvernamentală poate realiza în mod legitim supravegherea cetăţenilor statului respectiv şi a eventualelor limite ale unei astfel de supravegheri.

În Statele Unite această discuţie tinde să fie purtată în termeni de drept constituţional. De exemplu, se ridică problema modului în care ar

trebui interpretată, în cazuri ce privesc siguranţa naţională, interdicţia conţinută în cel de-al patrulea Amendament la Constituţia americană38 referitoare la percheziţii şi confiscări nejustificate. Se punea şi problema legitimităţii interceptării comunicaţiilor telefonice (care sunt considerate o formă de percheziţie) în cazuri ce ţin de

HăifiiH (a naţională: în cazul acestor interceptări realizate din raţiuni

* nipuianţă naţională, trebuie aplicată cerinţa obţinerii în prealabil I uimii mandat judecătoresc? Această întrebare şi-a găsit răspunsul im I cgea din 1978 privind informaţiile externe (FISA). În această» i era prevăzută condiţia obţinerii în prealabil a unui mandat Jwuv» aiuresc pentru interceptări în cazurile de siguranţă naţională, se înfiinţa o instanţă specială care emitea astfel de mandate şi Mff funcţiona conform unor proceduri menite să protejeze confiden-itoliiaica întregului proces39. În 1994 s-a introdus o procedură similară (naiiiu percheziţiile corporale în cazuri de siguranţă naţională40.

I»rei s-a acordat o atenţie deosebită acceptării sau neacceptării»lilri iiclor mijloace de derulare a activităţii de contrainformaţii (mijloace ilripre care nu vom discuta în detaliu aici), au fost neglijate o serie»I» probleme esenţiale privind scopurile activităţii de contrainformaţii nu ale activităţii serviciilor de informaţii interne într-o societate uYinocratică.41 Cu alte cuvinte, ce fel de informaţii sunt necesare? i r scop deservesc aceste informaţii? Ce tipuri de ameninţări impun Icslaşurarea acţiunilor de culegere a informaţiilor

pe plan intern?

liste foarte dificil de găsit un răspuns la aceste întrebări atunci lud este vorba de un stat democratic, spre deosebire de un stat cu intim totalitar. În acest din urmă caz, orice opoziţie la adresa h inducerii de stat constituie, în principiu, un element de interes pentru activitatea de informaţii. Monitorizând în mod constant opo-/ipa, conducerea statului se asigură că ia toate măsurile necesare pentru a rămâne la putere, fie prin intermediul sistemului obişnuit de iphcare a legii, fie prin mijloace din afara acestui sistem.

De asemenea, într-un stat democratic, simpla opoziţie faţă de ««inducerea statului de la un anumit moment dat nu este şi nu trebuie considerată o ameninţare la adresa ţării sau a sistemului ei de guvernământ. Interesele de securitate naţională ale unei ţări (spre deosebire de interesele de ordin politic ale conducerii statului) nu unt ameninţate de simpla existenţă a opoziţiei şi nu se impune desfăşurarea unei activităţi de culegere a informaţiilor pe plan intern» îi privire la aceste aspecte. Se pune atunci întrebarea: care sunt acţiunile ce constituie potenţiale ameninţări la adresa siguranţei naţionale şi impun culegerea unor informaţii în această privinţă?

În special, unde trebuie trasă linia de demarcare între acţiunile «are fac obiectul legitim al activităţii de culegere a informaţiilor şi cele lipsite de legitimitate? Activitatea de informaţii trebuie la albi în vedere opiniile propriu-zise ale unei persoane sau doar situaţttli în care aceste

opinii sunt însoţite de acţiuni? Criteriul ar trebui M fie acela al legalităţii sau ilegalităţii acţiunii? Există acţiuni uafti deşi sunt legale, trebuie să fie cunoscute de către conducerea statului şi, în consecinţă, pot fi supravegheate într-un fel sau altul?

*Standardul în materie de infracţionalitate*. Datorită al mp» prioritare acordate *mijloacelor* utilizate în culegerea informaţiilor *p* plan intern (mai ales în privinţa constituţionalităţii sau neconsi iiuţie, nalităţii acestor mijloace), în detrimentul *scopurilor*, aceste problem* nu au fost abordate în mod explicit în dezbateri publice privind activitatea de informaţii. Totuşi, s-a dat oarecum un răspun* l mijlocul anilor ’70, în Statele Unite (în perioada de desfăşurare A investigaţiilor privind activitatea de informaţii la nivelul Congresului) s-a încercat atunci aplicarea a ceea ce s-a numit „standardul în materie de infracţionalitate” în activitatea serviciilor de informaţii interne. Cu alte cuvinte, investigaţiile specifice serviciilor de inlormaţii interne se declanşau doar atunci când avusese sau urma să albi loc o încălcare a legii. Consecinţa a fost că obiectul de activitate al serviciilor de informaţii interne urma să fie delimitat de lege; îl acţiune ilegală poate constitui obiectul activităţii de culegere a informaţiilor, dar o acţiune legală nu poate face obiectul unor astfel de cercetări42. Deşi acest principiu nu a fost niciodată promovai într-o manieră foarte explicită, el a deschis calea recomandărilor date de Procurorul General în 1976. Impactul acestui principiu poate fi observat

şi în textul Legii din 1978 privind informaţiile externe, singurul act legislativ adoptat de Congres în acest domeniu în perioada respectivă43.

Aceste recomandări au fost date de Edward Levi, Procurorul General al Statelor Unite din perioada respectivă, precizându-se situaţiile în care FBI putea utiliza diferite tehnici de supraveghere şi investigare. În scopul elaborării acestor recomandări, domeniul informaţiilor interne a fost împărţit în două zone: securitatea internă, pe de o parte, şi informaţiile externe şi contrainformaţiile, pe de alin parte; au fost emise recomandări diferite pentru investigaţiile aferente fiecăruia dintre aceste domenii.

Recomandările pentru investigaţiile din domeniul informaţiiloi externe şi al contrainformaţiilor sunt clasificate şi nu au fost niciodată

Unite publice în totalitate”. De aceea, este dificil de stabilit în ce henna aceste recomandări aplică standardul în materie de infrac-pt Muriiiaic în cadrul investigaţiilor în care sunt aplicabile. Majoritatea Irigaţiilor realizate în baza acestor recomandări privesc identificarea *v* pirvenirea acţiunilor de spionaj. Astfel, investigaţiile se concentrează Apia activităţilor cu potenţial de infracţionalitate. Acelaşi lucru nit» valabil pentru depistarea şi prevenirea acţiunilor teroriste desfăluirtir sub comandă externă, aceasta constituind probabil cealaltă minune prioritară a FBI care trebuie îndeplinită conform reco-aMi îi în îi lor.

Nu este clar în ce măsură recomandările au

în vedere investigarea

* punilor politice legale desfăşurate în numele unui guvern străin, şi mume desfăşurarea unor acţiuni secrete sau măsuri active luate de an guvern străin şi îndreptate împotriva Statelor Unite. Este adevărat

1. În conformitate cu recomandările:

*cu respectarea standardelor şi procedurilor aprobate prin aceste intrornandări,* FBI este autorizat să depisteze şi să prevină acţiunile de pionaj, sabotaj şi *alte acţiuni clandestine de informaţii* derulate de puteri străine sau sub îndrumarea acestora, prin operaţiuni legale de «outrainformaţii desfăşurate pe teritoriul Statelor Unite, inclusiv prin supraveghere electronică, operaţiuni care sunt necesare sau utile în vederea atingerii obiectivelor45.

Aceasta înseamnă că activităţi în general legale, cum ar fi proi»u anda politică, acţiunile desfăşurate de diverse organizaţii şi nketarea unor fonduri, fac obiectul supravegherii atunci când sunt i.ilizate de o putere străină sau sub îndrumarea acesteia. De asemenea, cel puţin teoretic, oricine desfăşoară o astfel de activitate în mmele unui guvern străin este obligat să se înregistreze ca agent nain, în conformitate cu Legea de înregistrare a agenţilor străini îl aRA), neînregistrarea fiind o infracţiune".

În schimb, neînregistrarea nu constituie decât rareori singurul motiv pentru care se declanşează o investigaţie a serviciilor de i uiirainformaţii sau se începe urmărirea penală47. Probabil că singura investigaţie de acest gen a

privit Comisia pentru solidaritate cul»i»porul din El Salvador (CISPES), care a făcut obiectul unei verificări leiulate de FBI timp de trei luni în 1981. Investigaţia a avut loc la ei crea Direcţiei penale a Departamentului de Justiţie „pentru a stabili dacă CISPES trebuie să se înregistreze conform" legii i ah ca agent al Frente Democratico Revolucionario, aripa politică a mittfef de gherilă din El Salvador48. Având în vedere însă că acesta a sunt în *caz* excepţional, este neclar (cel puţin prin prisma infottuahbl publice disponibile) în ce măsură standardele şi procedurile aphtfefli prin aceste recomandări permit o investigare eficientă a activitjtylki clandestine de informaţii care nu implică violenţă sau înciltUM vreunei legi (alta decât FĂRĂ).

Spre deosebire de recomandările privind activitatea de rotai a informaţii, cele referitoare la securitatea internă (denumite „reconwiiilirli Levi") au fost făcute publice49. Acestea privesc, în primul titit investigarea grupărilor care au fost denumite la un moment lit „subversive" sau „antiamericane". Deşi aceşti termeni sunt imprtt i*«se includ aici grupări: (1) ostile nu doar guvernului aflat la piu» şi politicilor acestuia, ci şi structurii constituţionale şi principiului sale fundamentale, (2) grupări care urmăresc încălcarea dreptul lltil civile ale anumitor categorii de persoane (cum ar fi grupurile raiul» etnice sau religioase) sau (3) grupări ce urmăresc înlăturarea ton ducerii politice prin mijloace violente.

Elementul-cheie al recomandărilor lui Levi este că investigata! activităţii acestor grupări e

permisă doar atunci când o grupare (iau un individ) este implicată sau se poate implica în activităţi „tata presupun sau vor presupune utilizarea forţei ori a violenţei şi caii presupun sau vor presupune încălcarea legislaţiei federale” 50. Acehă este, în esenţă, standardul în materie de infracţionalitate, care stabiles cu claritate sfera de interes a guvernului în domeniul securităţii interne

Cel mai important motiv pentru adoptarea acestui standard a ftart garanţia că nu se întreprinde nicio acţiune de supraveghere doar pentru că o persoană sau un grup îşi exercită dreptul de liberi exprimare, dreptul libertăţii presei sau cel de liberă asociere, prevăzttta în Primul Amendament la Constituţia Statelor Unite51. Există doul argumente care justifică acest obiectiv. În primul rând, există opinia potrivit căreia o investigaţie guvernamentală întreprinsă asupra unei persoane sau a unui grup constituie în sine o sancţiune ce nu ai trebui să li se aplice celor care nu au comis nicio ilegalitate. (el de-al doilea argument evidenţiază faptul că acest tip de investigaţie, fie din cauza caracterului său neplăcut pentru cel vizat, fie din cauză că pare să anunţe o pedeapsă ulterioară, „îngheaţă” în mod inevitabil

Mit Halca (exercitarea dreptului) care face obiectul supravegherii, te«it motive sunt plauzibile într-o anumită măsură, dar nu sunt pm.i«, una foarte convingătoare. În termeni constituţionali, se pune liiri Mi ca dacă supravegherea realizată în asemenea condiţii reprezintă PINiiAiigere a

libertăţilor garantate de Primul Amendament.

A* castă problemă nu poate fi tratată aici pe larg. Câteva elemente îniim/a însă argumentele pro şi contra adoptării standardului în lunule de infracţionalitate. Pe de o parte, încălcarea dreptului la MA pl, ivată, pe care o presupune urmărirea unei persoane de către ignipile guvernamentale, este într-adevăr dezagreabilă. Totuşi, Ştiuţi lucru este valabil pentru toate investigaţiile întreprinse de – linkânsărcinate cu aplicarea legii care vizează persoane ce nu unui suspectate de a fi comis o anumită infracţiune: verificările tivind impozitul pe venit, inspecţiile vamale şi multe alte acţiuni «i. În ganelor responsabile de aplicarea legii constituie un amestec în mia privată, dar guvernul este autorizat şi chiar întreprinde astfel a. măsuri fără a avea motive să suspecteze că persoana vizată a mis vreo infracţiune. De asemenea, posibilitatea unei supravegheri întreprinse de către intuiţiile guvernamentale ar putea să descurajeze activităţile politice

…iioversate, deoarece ar exista temerea că includerea numelor jM i.nanelor implicate într-un dosar ar putea crea probleme în viitor, lotuşi, efectul restrictiv al unei investigaţii secrete care nu se finalizează prin întreprinderea unei acţiuni nu poate fi decât unul minim! li-i tul pare să fie mai degrabă echivalent oprobriului public pe care în persoană şi l-ar atrage dacă ar îmbrăţişa idei lipsite de popularitate, li i al cel de limitare a libertăţilor prevăzute în Primul Amendament, hmivit dreptului constituţional, Curtea Supremă a

respins opinia, inform căreia o persoană are de suferit ca urmare a „simplei

Mstenţe a unei acţiuni guvernamentale de investigaţii şi de culegere unor informaţii”. Curtea a hotărât că, în ceea ce priveşte îndeplinirea condiţiilor legale pentru a contesta o investigaţie guvernamentală în l.iţa instanţei, „afirmaţiile privind efectul restrictiv subiectiv [ca în mare a desfăşurării unei investigaţii guvernamentale secrete] nu i h»I substitui în mod adecvat existenţa unei vătămări concrete, obiective „au riscul produceri unei astfel de vătămări în viitor” 52.

Aşa cum remarca Kenneth Robertson, această problemă este i Ic/bătută, în general, din punctul de vedere al interdicţiilor prevăzute de dreptul constituţional cu privire la anumite tipuri de hi \ *Um* guvernamentale. De asemenea, trebuie să se analizeze dac A m* standarde permit guvernului să îşi satisfacă nevoile legitima É informare cu privire la evenimentele ce au loc în societatcă* (li «H puţin două domenii de interes, se poate argumenta că, măcar în am, aceste standarde nu acordă guvernului suficientă libertate de atiţl Wţ

*Standardul în materie de infracţionalitate şi securitatea personalul** Primul dintre aceste domenii priveşte programul guvernului de a-ia» rare a securităţii personalului, menit să verifice potenţialii sau actualM angajaţi guvernamentali înainte de a le acorda acces la informaţii clasificate. În acest scop, guvernul este îndreptăţit să ştie iM* «respectivii candidaţi au afilieri sau legături care i-ar putea determini să le divulge

informaţii clasificate reprezentanţilor unor puteri sii Ali» sau să acţioneze în alt mod împotriva intereselor ţării. În general aceste aspecte sunt dificil de stabilit în cadrul verificărilor, am motivele enumerate în capitolul 5. Singura posibilitate ca cu venait să poată afla cu o anumită certitudine dacă respectivul candidul ah o astfel de afiliere este ca instituţiile guvernamentale să aibă şi alta surse de informaţii provenind din supravegherea organizaţi Unt respective.

În această privinţă, este important să înţelegem în ce anutlli constă protecţia asigurată de Primul Amendament. Conform hotăr Aill Curţii Supreme în cazul *Brandenburg vs Ohio*, este protejată „suiţi nerea la nivel teoretic" a ideii răsturnării guvernului american Susţinerea unor astfel de idei poate fi interzisă doar atunci cătal „aceste idei sunt menite să incite sau să provoace acţiuni anarhist! *iminente* şi există probabilitatea incitării sau provocării unor asllal de acţiuni" 54. Conform unui standard strict în materie de infracţinnalitate, o organizaţie care încurajează răsturnarea prin violenţa a Guvernului american nu poate face obiectul supravegherii decât! atunci când acţiunile sale trec de la nivelul abstract la cel concrd, aşa cum am explicat mai sus.

În plus, apartenenţa la o organizaţie care desfăşoară acţiuni concrete de promovare poate avea caracter de infracţionalitate doar dacă persoana respectivă este membru activ şi dacă are „cunoştinţa despre activitatea ilegală de promovare desfăşurată de organizaţie şi dacă are intenţia clară de a provoca răsturnarea prin

violenţă a

I Hivc Tiiului american «cât mai repede posibil în circumstanţele date»M w, \.i lucru înseamnă că, dacă s-ar respecta un anumit standard lui RMlerie de infracţionalitate, ar fi imposibilă supravegherea unei Htnenea organizaţii în vederea elaborării unei liste complete a Htiunbrilor săi, din moment ce nu ar exista probe care să demonstreze i A flecare dintre membrii organizaţiei se încadrează în standardul de lühacţionalitate, chiar dacă organizaţia, în ansamblu, corespunde» lleriului *Brandenburg*.

Într-o oarecare măsură, imposibilitatea realizării unor liste cu numele membrilor organizaţiilor „subversive" (acele organizaţii care, «Iute fiind obiectivele lor, pun sub semnul întrebării capacitatea membrilor de a obţine acces la informaţii clasificate) a fost rezultatul urmărit prin adoptarea standardului în materie de infracţionalitate. Ayi cum remarca John Elliff, prezentând deciziile iniţiale ale hncurorului General al SUA Edward Levi:

Levi a respins ideea că programul de securitate pentru angajaţii din structurile federale poate constitui baza investigaţiilor informative realizate de FBI. După părerea lui Levi, decretul (privind programul de securitate a personalului) autoriza Biroul doar să investigheze angajaţii şi candidaţii pentru executiv. Decretul nu constituia temeiul în baza căruia FBI să poată desfăşura investigaţii informative pe plan intern56.

Cu alte cuvinte, investigaţiile nu pot porni de

la acţiunile sau declaraţiile publice ale unui grup. Ele trebuie să înceapă doar dacă există o solicitare de ocupare a unui post în structurile administrative din partea unei persoane a cărei afiliere la o grupare poate fi camuflata.

Fără a supraveghea astfel de grupări în scopul întocmirii unei liste a membrilor lor, guvernul federal nu poate, în general, să ia măsurile necesare pentru a avea certitudinea că nu acordă acces la în formaţii confidenţiale sau nu numeşte în posturi importante peroane care sunt membre ale unor partide politice loiale unei puteri străine ostile, membre ale unor grupări religioase ce dau dovadă de nu devotament fanatic pentru liderii lor, ale căror scopuri reale ar putea să nu fie compatibile cu ideea de guvernare constituţională sau membre ale unor grupări ostile ce vor să excludă anumite categorii de cetăţeni americani din rândul clasei politice. Acest lucru poate sau nu să reprezinte o problemă la un moment dat, în funcţie de existenţa unor astfel de grupări şi de măsura în care acestea sunt capabile să elaboreze o strategie menită să ascundă legătura meinhi în lor cu gruparea şi să îi plaseze în funcţii guvernamentale imporim”* („infiltrându-se” în guvern) 57.

*Standardul de infracţionalitate şi antiterorismul*. Situaţia Me întrucâtva diferită în cazul grupărilor teroriste. Deşi o grupul* teroristă activă poate face obiectul supravegherii indiferent de m.m dardul de infracţionalitate aplicat, poate fi extrem de dificilă institulff Mi unei astfel de supravegheri în cazul unor grupări sofisticate, aşa

cum sunt majoritatea grupărilor teroriste care au apărut în ultimele decpitll în Orientul Mijlociu şi Europa Occidentală. Având în vedere cai de puţine informaţii pot fi obţinute prin mijloace tehnice cu privire li locaţiile stabile şi mijloacele de comunicaţie ale acestor grupări, de mai utilă tehnică de culegere a informaţiilor este infiltrarea unot agenţi într-o grupare. O grupare sofisticată va fi însă precaută QU privire la persoanele din afară şi va avea încredere doar în acel, persoane cu care membrii actuali au avut relaţii personale îndelungul* sau care şi-au dovedit devotamentul faţă de grupare prin comitere* unor infracţiuni grave. Doar şansa poate ajuta un serviciu de infotmaţii ca, pornind de la zero, să îşi infiltreze agenţii într-o grupare teroristă deja organizată şi operaţională.

Serviciile de informaţii trebuie să recurgă la alte strategii pentru a rezolva această problemă. În primul rând, serviciile trebuie să poată culege informaţii despre grupurile de sprijin – simpatizaşi care asigură susţinere financiară, logistică, politică şi juridică, dat nu iau parte la activităţile teroriste propriu-zise.

Infiltrarea într-un grup de sprijin, deşi mai simplu de realizat, nu este la fel de avantajoasă ca infiltrarea în gruparea teroristă. Cu toate acestea, ea poate fi foarte utilă; în funcţie de tipul sprijinului acordat, se pot deduce momentul şi natura unor viitoare acte teroriste. În plus, un membru al unui grup de sprijin, prin legăturile sale personale sau prin recrutarea de către gruparea teroristă, poate ajunge într-o poziţie din

care să furnizeze informaţii mai exacte. Un agent infiltrat într-un grup de sprijin poate fi în măsură să împiedice comiterea uni act terorist, fie furnizând poliţiei o informaţie-cheie (cum ar fi descrierea maşinii închiriate care urmează să fie utilizată în actul terorist), fie sabotând direct atentatul cu bombă (de exemplu, înlocuind praful de puşcă cu rumeguş) sau alte echipamente. Aşa

— Mim explica Shlomo Gazit, fost director al Direcţiei de Informaţii Militare israeliene, Aman:

Sunt foarte puţine organizaţiile [teroriste] care pot funcţiona într-un sistem de compartimentare totală şi care nu depind de reţele locale de sprijin. Aceste reţele sprijină organizaţia teroristă fie din raţiuni ideologice, lie ca urmare a unor acţiuni de intimidare şi şantaj, fără a se implica direct în operaţiunile teroriste. Importanţa infiltrării în reţelele de simpatizanţi şi susţinători rezidă în faptul că aceasta este mult mai simplu de realizat decât infiltrarea în organizaţiile teroriste, care sunt mai greu accesibile. Infiltrarea în aceste reţele de sprijin poate face posibilă infiltrarea în organizaţia propriu-zisă sau obţinerea unorinformaţii indirecte despre aceasta58.

Standardul în materie de infracţionalitate împiedică infiltrarea în pânpurile de sprijin deoarece acestea se prezintă în general sub forma unor grupări politice sau caritabile, ceea ce şi sunt, într-o anumită măsură. Un grup de sprijin poate susţine că este implicat în acţiuni de propagandă politică în favoarea unor cauze care sunt, întâmplător, îmbrăţişate şi de gruparea

teroristă. În mod similar, alt grup poate susţine că activitatea sa are ca scop sprijinirea soţiilor şi copiilor unor presupuşi terorişti care au fost închişi sau ucişi. Un alt grup poate susţine că se limitează la asigurarea asistenţei juridice şi a rondurilor necesare pentru apărarea teroriştilor puşi sub acuzare.

Fără infiltrarea unui informator în grupul de sprijin, ar putea fi imposibil să se stabilească natura exactă a activităţilor secundare (şi deloc inocente) desfăşurate de grupul de sprijin în numele organizaţiei teroriste. Dar utilizarea unei asemenea metode intruzive sau a altei tehnici similare este permisă doar dacă există deja dovezi privind implicarea grupului în acţiuni violente, infracţionale59. În această privinţă, standardul în materie de infracţionalitate creează un cerc vicios: nu se pot cunoaşte activităţile secundare desfăşurate de un grup pentru că nu pot fi investigate şi nu pot fi investigate deoarece nu există informaţii despre derularea unor astfel de activităţi.

O a doua modalitate de depăşire a problemei legate de supravegherea grupărilor teroriste se bazează pe faptul că ele sunt, în general, ramuri ale grupărilor extremiste, naţionaliste sau separatiste; ele sunt alcătuite, de obicei, din membri ai unor astfel de grupări, nemulţumiţi de faptul că nu reuşesc să îşi atingă obiectivele prin mijloace mai puţin violente. Prin infiltrarea unor informatori în rândul organizaţiilor din care se pot desprinde grupări teroriste, Mit posibil să se cunoască imediat existenţa unei noi grupări

tenului» ţ să se infiltreze agenţi în cadrul acestora încă de la început. În sclilinh un standard în materie de infracţionalitate face imposibilă mai lui» n supravegherii iniţiale, pe baza căreia pot fi obţinute primele indu în referitoare la o nouă grupare teroristă.

O componentă aparte a activităţii de combatere a terorismului n reprezintă responsabilitatea serviciului secret american de a asigurl protecţia preşedintelui, a altor înalţi demnitari, precum şi a ctitn străini. Scopul acestei activităţi, ca, de altfel, al întregii activităţi de combatere a terorismului, constă mai degrabă în a preveni un ««criminal decât în a riposta la o astfel de acţiune prin pedepalrn făptuitorilor, astfel încât să se evite viitoare acţiuni de acest goii Responsabilitatea serviciului secret presupune deţinerea unor informaţii despre posibile tentative de asasinat care vizează persoanele alint* sub protecţia sa. Standardul în materie de infracţionalitate aplicabil în cazul investigării grupărilor care pot fi implicate în asasinul* presupune că serviciul secret nu va primi avertizări cu privire la posibile tentative de asasinat decât după ce gruparea a iniţiat deja n acţiune violentă, moment în care deţinerea acestor informaţii ut putea fi tardivă. În 1982, un oficial din cadrul Departamentului Trezoreriei, responsabil de relaţia cu serviciul, a explicat problema astfel: „În ziua de azi, serviciul secret trebuie să manifeste preocu pare faţă de intenţiile şi activităţile grupărilor teroriste sau ale altoi grupări extremiste. Trebuie să cunoaştem acest

tip de ameninţare înainte ca ea să se materializeze, nu după aceea” 60.

De asemenea, oficialul a remarcat faptul că, pentru o alocare adecvată a resurselor, serviciul trebuie să „ştie că, de exemplu, o organizaţie ce are un discurs extremist fie nu are disponibilitatea necesară transpunerii în practică a mesajului său, fie este incapabilă să declanşeze acţiuni periculoase”. În opinia sa:

…problema actuală este că FBI nu este capabil să culeagă suficiente informaţii, lucru care se datorează, în parte, recomandărilor privind securitatea internă, promovate de Procurorul General al SUA, Levi Anterior emiterii acestor recomandări, serviciul secret primea de la FBI numeroase informaţii secrete despre anumite persoane şi grupări care puteau recurge la acte de violenţă. Deşi s-a considerat că, în felul oesta, serviciul secret a beneficiat de prea multe informaţii Imul im voit să facă o selecţie dintr-un volum mare de informaţii –, situaţia ora Ideală din punctul său de vedere.

Ai mula problemă constă în faptul că nu se realizează o serie de investigaţii în anumite domenii importante. Rezultă de aici o lipsă de informaţii îi lentoare la locaţia, structura, planurile şi activităţile unor grupfiri».11 e nu pot fi etichetate drept teroriste, dar care au o orientare radicală, sprijină cauzele organizaţiilor teroriste şi pot recurge la acţiuni violente, au teroriste.

I) csigur, această abordare generală este valabilă în cazul tuturor Agenţiilor responsabile de

aplicarea legii; în general, activitatea a» estor agenţii vizează doar în mică măsură prevenirea infracţiunilor, i concentrându-se asupra depistării activităţilor infracţionale după, omiterea lor şi asupra pedepsirii autorilor. Este imposibil ca agenţiile obişnuite responsabile de aplicarea legii să îşi stabilească drept obiectiv prevenirea infracţiunilor, prin crearea unei reţele informative» are să le avertizeze în legătură cu plănuirea unor acţiuni infracţionale, în ceea ce priveşte combaterea terorismului şi protecţia demnitarilor, din cauza gravităţii pe care o poate avea chiar şi un singur incident, există mai multă disponibilitate de a preveni infracţiunile, şi nu doar de a le sancţiona, fapt ce implică necesitatea culegerii unor informaţii despre persoane sau grupări ce, deşi nu au comis acţiuni violente, pot să se implice în astfel de activităţi sau să menţină legături strânse» u cei care comit astfel de acţiuni.

În 1995, în urma atentatului cu bombă asupra sediului FBI din o klahoma City, care s-a soldat cu un număr mare de victime, s-a pus «Im nou întrebarea dacă recomandările în materie de combatere a terorismului pe plan intern conferă FBI suficiente competenţe. Totuşi, rrocurorul General, Janet Reno, şi Louis Freeh, directorul FBI, au considerat că revizuirea acestor norme nu este necesară, anunţând că prevederile în vigoare la momentul respectiv (recomandările lui Levy fuseseră revizuite de Procurorul General, William French Smith, în 1983) urmau să beneficieze de o interpretare mai puţin restrictivă; prevederile respective stabileau posibilitatea declanşării unei

inves-ligaţii pe probleme de antiterorism atunci când, „în baza faptelor şi împrejurărilor existente, se poate trage concluzia că două sau mai multe persoane sunt implicate într-o acţiune care vizează atingerea unor obiective politice sau sociale prin utilizarea forţei ori a violenţei şi nerespectarea legislaţiei penale a Statelor Unite” 61. Potrivii $ Freeh, această reinterpretare avea să „permită FBI să demaffe investigaţie în cazul unei grupări ce recurge la violenţă pentru §*A* atinge obiectivele politice sau sociale, fără a încălca însă legliltpi federală, dacă există indicii că respectiva grupare are capacitatea tit a-şi atinge scopurile” 62.

Deşi criteriul existenţei unor „indicii temeinice” este sufleifrti *M* general pentru a include şi interpretarea lui Freeh (potrivit căror NU trebuie să existe neapărat date privind o încălcare iminentă a leg în el presupune mai mult decât promovarea „abstractă” a violons într-adevăr, potrivit recomandărilor aprobate de Smith, acest criteriu necesită luarea în calcul a dimensiunii, probabilităţii şi iminenţii ameninţării (care trebuie analizate în raport cu „impactul unei investigaţii asupra vieţii private şi libertăţii de exprimare”) 63. De aceea, dffl această reinterpretare nu mai impune necesitatea existenţei unor dovezi privind o „iminentă” încălcare a legii, ea se menţine în spiritul „standardului în materie de infracţionalitate”.

*Argumente în favoarea standardului în materie de infracţionalitau* Este mai uşor să se aducă argumente teoretice împotriva standardului

în materie de infracţionalitate aplicabil în cazul investigaţiilor din domeniul securităţii interne decât să se identifice un substitui Standardul a fost adoptat după ce Comisia Church a documentat mai multe cazuri în care FBI a desfăşurat investigaţii ce au implicat al At utilizarea unui volum exagerat de resurse, cât şi amestecul nejustifica! în activităţi politice care nu prezentau riscuri la adresa securităţii naţionale. Această implicare excesivă, aşa cum a denumit-o Comisia Church, a reprezentat un argument în favoarea adoptării unul standard clar care să limiteze numărul investigaţiilor la cele imperiu* necesare. Investigaţiile necesare au fost definite drept acelea care vizează acte infracţionale însoţite de violenţă ce au avut loc sau urmează să se producă.

Cazurile de implicare excesivă în investigaţiile din domeniul securităţii naţionale se încadrează în mai multe categorii. Probabil cele mai evidente au fost cazurile în care, la solicitarea Casei Albe, FBI a desfăşurat investigaţii cu privire la adversarii politici ai preşedintelui. Laurence Silberman, judecător şi fost adjunct al Procu rorului General, a declarat în 1978 că, „dintre toate abuzurile comise diverse agenţii guvernamentale în ultimii 20 de uni, am! lă ifei/ul cel mai revoltător a fost cel al preşedintelui Johnaon, biff A Inlmnat FBI să încerce să afle informaţii compromiţătoare deapte»iiui senatorului Barry Goldwater, cu două săptămâni înainte de ikgerile prezidenţiale din 1964”64. Există şi alte cazuri similare în taie să apelat la

FBI pentru discreditarea adversarilor politici din
4 i! ml Congresului, a unor jurnalişti sau a altor persoane.

În multe alte cazuri, investigaţiile au avut ca obiect grupări politice militante, cum ar fi:

grupări „de dreapta” sau „extremiste” angajate în „lupta anticomunistă”; grupări „anarhiste sau revoluţionare”;

…naţionalişti de culoare” şi „extremişti”; grupări care promovează „supremaţia rasei albe”;

„Agitatori” 65.

În aceste cazuri, deşi se pare că a existat o corelaţie între organizaţiile investigate şi anumite acţiuni violente sau legături cu servicii secrete nu Aine, investigaţiile desfăşurate au fost mult prea extinse în ceea ce ia iveşte numărul persoanelor şi grupărilor vizate, informaţiile tan genţiale culese despre ele şi perioada de timp alocată acestor investigaţii lipsite de perspective. Informaţiile tangenţiale obţinute au fost reţinute în dosarele de anchetă şi, totodată, diseminate în latinii guvernului; în felul acesta, administraţia a putut utiliza în i opuri partizane informaţiile despre activităţi politice legitime care au fost puse la dispoziţia sa”.

Pornind de la concluziile Comisiei Church, este evident că excesele au fost facilitate de absenţa unor standarde precise în domeniul investigaţiilor informative desfăşurate pe plan intern. Prin urmare, este uşor de înţeles de ce un standard în materie de infracţionalitate reprezintă o soluţie clară şi atractivă. Dacă acesta are un caracter prea restrictiv, trebuie identificată o

alternativă mai cuprinzătoare, i are să nu mai permită însă repetarea abuzurilor din trecut.

Acest lucru nu se poate realiza rapid. Pentru a aborda situaţia într-o manieră responsabilă, trebuie să se stabilească, iniţial, activităţile politice sau de altă natură desfăşurate pe plan intern pe care un guvern democratic este îndreptăţit să le cunoască, astfel încât să fie în măsură să prevină eventualele ameninţări. În SUA, legistul) * deciziile executivului şi normele din domeniul informaţiilor imn im au fost concepute din perspectiva condiţiilor ce trebuie îndeplinir anterior aplicării diferitelor tehnici de investigaţie. Pe de o parte, tui există prevederi oficiale cu privire la obiectivul activităţii de informaţii desfăşurate pe plan intern sau la tipul informaţiilor ce ar trebui îi rezulte din această activitate. Numai existenţa unor astfel de prevedei I va permite elaborarea unor norme care pun accent pe obiectivul activităţii de informaţii (ce tipuri de informaţii sunt necesare), Iu detrimentul mijloacelor utilizate (tehnicile de investigaţii utilizate!

Legislaţia canadiană, pe de altă parte, defineşte ameninţările u» care trebuie să le gestioneze agenţia ce desfăşoară activităţi de informaţii pe plan intern, Serviciul Canadian de Informaţii privitul Securitatea (Canadian Security Intelligence Service – CSIS). El oMl autorizat să culeagă informaţii despre activităţi „în legătură cu cure există dovezi pertinente potrivit cărora acestea pot constitui o ameninţare la adresa securităţii Canadei”. Aceste activităţi sunt definite

astfel:

spionaj sau sabotaj ori alte activităţi care vizează sau vin în sprijinul actelor de spionaj sau de sabotaj; activităţi sub influenţă străină de natură să aducă atingere intereselot Canadei şi care sunt clandestine, au scop de dezinformare muu implică o ameninţare la adresa unei persoane; activităţi care vizează sau vin în sprijinul ameninţării oriul recurgerii la violenţă pentru atingerea unor scopuri politice; activităţi care vizează sau sunt menite să conducă la răsturnare» prin mijloace violente a guvernului canadian67.

Chiar şi în condiţiile unei definiri adecvate a obiectului activităţii de informaţii desfăşurate pe plan intern, se pune întrebarea dacă o anumită grupare constituie o ameninţare sau are doar un discut» exacerbat şi care sunt volumul şi tipul dovezilor necesare pentru CA o grupare să fie considerată o ameninţare ce trebuie avută în vedere Fără a înţelege exact ce informaţii privind securitatea naţională sunt necesare, este imposibil de apreciat dacă se justifică anumite restricţii aplicabile mijloacelor de investigaţie.

Capitolul 7

Două perspective asupra lumii informaţiilor în precedentele cinci capitole am analizat cele patru elemente ale iuţivităţii de informaţii – cele patru categorii de activităţi informa-iive –, precum şi anumite aspecte privind relaţia dintre serviciile de informaţii, pe de o parte, şi celelalte structuri guvernamentale şi omponente ale societăţii, pe de altă parte. Acum, vom aborda şi I»i i) l) lema

generală a naturii activităţii de informaţii în ansamblu, începând pilii a face o comparaţie între aşa-numita „viziune tradiţională asupra cultivităţii de informaţii” (care pune accentul pe obţinerea, protejarea) \ valorificarea informaţiilor secrete cu relevanţă în relaţiile dintre iuliuni) şi viziunea mai recentă, tipic americană, asupra activităţii uv informaţii, care s-a conturat după cel de-al Doilea Război Mondial.

Într-o anumită măsură, viziunea „tradiţională” prezentată aici ne aparţine. Deşi ea reflectă conceptele tradiţionale ale activităţii de informaţii, ele nu au fost formulate de regulă în această manieră. { Trebuie reamintit faptul că, în trecut, nu s-au publicat multe lucrări pe tema activităţii de informaţii.) Această viziune este utilizată aici i-a termen de comparaţie menit să evidenţieze caracteristicile viziunii americane care a apărut după cel de-al Doilea Război Mondial.

Viziunea „tradiţională” îşi are originea în una dintre cele mai vechi analize pe tema activităţii de informaţii, o carte clasică, *Arta Războiului*, a tisă de Sun Tzu, general şi strateg militar chinez din secolul al VI-lea i I În Faţă cum a explicat el importanţa activităţii de informaţii:

Motivul pentru care prinţul luminat şi generalul înţelept îşi învinq duşmanii de fiecare dată, iar izbânzile lor le depăşesc pe cele ale oamenilor de rând este previziunea.

Ceea ce numim „previziune” nu este un dar al spiritelor sau «I MMI nici nu rezultă prin analogie cu evenimente trecute ori în unu* mă calcule. Ea poate fi obţinută de la cei care cunosc situaţia

iikuu»…i – (altfel spus, cei care au acces în tabăra inamicului) 1.

Spionajul este elementul principal al acestei viziuni asupra acih nap? de informaţii. Dată fiind legătura strânsă dintre cunoaştereatelor duşmanului şi înfrângerea acestuia, este de la sine înţoli» e protejarea propriilor secrete (contraspionajul) este la fel de impoi i am «ca şi descoperirea secretelor adversarului. Sun Tzu identifică don't metode de a obţine acest rezultat:

atragerea agenţilor inamicului, prin lansarea unei oferte iimi avantajoase; trimiterea unor spioni în tabăra inamicului, care au fost indul în eroare cu privire la propria situaţie, astfel încât, dacă sunt capturaţi şi forţaţi să vorbească, să-l poată înşela fără a fi nici ei conştienţi de acest lucru2.

Scopul fundamental al spionajului îl reprezintă o foarte huuă înţelegere a strategiei inamicului, astfel încât planurile acestuia lă poată fi dejucate, iar el să poată fi învins, cu cele mai mici pierdeţi posibile. Din punctul de vedere al lui Sun Tzu, pentru care este mai important să dejoci strategia inamicului decât să învingi pe câmpul de luptă, componenta informativă este la fel de importantă ca şi cea militară:

De aceea, în război, cel mai important lucru este să dejoci strategia du* manului, apoi să-i distrugi alianţele, pentru ca, în final, să-i ataci armata1

Activitatea de informaţii este similară unui conflict armat, diferenţa constând în mijloacele utilizate.

Într-un articol care pledează pentru „dezvoltarea unui sistem de informaţii adecvat Statelor Unite”, fostul director CIA William Colby face o distincţie între un astfel de sistem şi sistemele de informaiit tradiţionale, pe care le descrie astfel:

Timp de secole, activitatea de informaţii a fost apanajul monarhilor şi generalilor. Spionajul guvernamental şi militar a scos la iveală secretele altor puteri, în scopul obţinerii unor avantaje. Agenţii secreţi au uneltii mmul a-i discredita pe inamici ori pentru a-i sprijini pe adveranrll lot în I din propria tabără. Spionul era prototipul acestei „discipline informative iiaililionale” 4.

(olby defineşte „conceptul tradiţional de *activitate de informaţii*” ftep»i „un serviciu secret care descoperă un plan secret al duşmanului ti i I dezvăluie monarhului, cu scopul ca acesta să poată câştiga Mifiha”\ El susţine că experienţa acumulată de Statele Unite în I* i loada celui de-al Doilea Război Mondial a dus la conturarea unei Httl viziuni asupra activităţii de informaţii, care se deosebea, în Mitvinţa unor aspecte fundamentale, de viziunea tradiţională. În h»noada postbelică, această viziune a continuat să capete contur, în rândul comunităţii de informaţii a Statelor Unite, cât şi în lumea academică. Prezentul capitol ia în discuţie această nouă viziune îl face o comparaţie între ea şi viziunea „tradiţională”.

Istoricul viziunii americane i lunarul instabil instaurat după izbucnirea celui de-al Doilea Război Mondial şi după intrarea Statelor Unite în război a dus la o sporire «mnificativă a resurselor

alocate de SUA activităţii de informaţii. I se asemenea, a condus la înfiinţarea unui serviciu central de informaţii (denumit iniţial Biroul de Coordonare a Informaţiilor şi ulterior Ituoul de Servicii Strategice sau OSS), care avea ca obiective culegerea, analizarea, precum şi centralizarea datelor şi informaţiilor privind securitatea naţională6. Deşi preşedintele Franklin Roosevelt a decis, în iulie 1941, înfiinţarea unui organism care să centralizeze informaţiile, agenţia respectivă nu a fost înfiinţată până în decembrie 1941, atunci când neanticiparea atacului japonez de la Pearl Harbor a evidenţiat deficienţele în materie de analiză şi centralizare a numeroaselor informaţii fragmentare ce erau disponibile.

Importanţa activităţii de analiză

O SS a înfiinţat un departament de cercetare şi analiză care urma „să analizeze toate informaţiile relevante, obţinute din surse deschise şi surse secrete” 7. Deşi acest ideal nu a fost atins în timpul celui de «M Doilea Război Mondial, aceasta s-a întâmplat, în cele din urmă A, pun înfiinţarea Agenţiei Centrale de Informaţii, CIA, în 19478.

Acest accent pe analiza informaţiilor, corelarea şi centrallii Èfi unor informaţii disparate în vederea conturării unei imagini că-l «incorecte sugerează o viziune asupra activităţii de informaţii di!» ime de cea „tradiţională”. Această nouă viziune acordă mai puţină atenţii confidenţialităţii, punând un accent deosebit pe funcţia analii un

Această viziune a fost promovată cu succes, imediat după închru i... celui de-al Doilea Război

Mondial, de către Sherman Kent, I«ofiţer OSS şi viitor şef al Biroului pentru Estimări Naţionale al (1 A«care, la vremea respectivă, avea ca sarcină întocmirea unor evalultl complete ale situaţiei internaţionale. Cunoscuta sa carte, *Informfô strategice pentru politica externă a SUA*, pleda pentru înţelegerii activităţii de informaţii ca metodă ştiinţifică (în varianta sa de ştiluă socială) aplicată problemelor strategice:

Noi, cei de tradiţie liberală, considerăm că cercetarea este singular proces care ne oferă adevărul sau ne apropie cel mai mult de adevif Insistăm – cum au făcut şi alte generaţii înaintea noastră – asupra faptului că adevărul trebuie obţinut printr-o cercetare bazată pe o metodă sistematic Există o astfel de metodă în cadrul ştiinţelor sociale, care reprezintă. În linii mari, esenţa activităţii strategice de informaţii. Această metodă le aseamănă în mare măsură cu cea a ştiinţelor naturale. Nu este aceeaşi metodă, dar, fără îndoială, e o posibilă metodă de lucru9.

Desigur, activitatea de informaţii nu se poate reduce la metodă ştiinţelor sociale, chiar dacă aceasta reprezintă o componentă eseuţială. La urma urmei, trebuie să existe date cărora să le poată fi aplicată. Deşi admite că anumite date trebuie obţinute prin mijloace clandestine, Kent susţine că viziunea tradiţională asupra activităţii de informaţii, care pune accent pe aspectul confidenţialităţii, este un mit. În opinia sa, analiza informaţiilor se poate baza pe date obţinute surse publice, la care se pot adăuga un număr redus de informait! obţinute din surse secrete. Referitor la

informaţiile necesare pentru elaborarea politicii externe – obiectul activităţii strategice de informaţii –, el afirmă: „Unele dintre aceste informaţii pot fi obţinute prin mijloace clandestine, *însă majoritatea trebuie obţinute prin activităţi de observare directă şi cercetare" 10*.

În lor mă sa extremă, această nouă viziune echivalează activitatea *h* inloimaţii cu un gen de ştiinţă socială, universală şi anticipativă 4 r iisită abordare a fost descrisă astfel de Colby în 1981:

I uhu le perfecţionată o nouă disciplină al cărei obiect specific de» «nvitate îl reprezintă analiza informaţiilor, iar procesul de cercetare şi h7 voltare a început deja. Această disciplină va merge mai departe dec, lt în iliza ştiinţifică, prin aplicarea unor noi tehnici de anticipare a unor venimente probabile, în detrimentul explicării evenimentelor trecute. I xpertinentele specifice acestei noi discipline nu se limitează la comuniunea de informaţii, având loc şi în centre de cercetare din domeniul Itiinţei informaţiilor, în mediul analiştilor care evaluează riscurile politice şi în cadrul previziunilor realizate de Clubul de la Roma, de mudiul Global 2000 şi de alte studii".

Importanţa analizei informaţiilor este o trăsătură definitorie a n «.tei noi viziuni asupra activităţii de informaţii. Pentru a înţelege îi. Îi bine această viziune, vom analiza argumentele pe care un adept îl acesteia le va invoca pentru a-l convinge pe un „tradiţionalist" de «levarul său. Se porneşte de la observaţia că, indiferent de viziunea iiipra activităţii de informaţii, trebuie recunoscut rolul său important el puţin în cazul

câtorva tipuri de analize.

În primul rând, activitatea de culegere informaţiilor generează imediat necesitatea analizei, fie tehnice (cum ar fi descifrarea mesa-i lor codificate), fie cu caracter general (cum ar fi compararea i ipoartelor din două surse diferite pentru a verifica dacă informaţiile

»meid sau se contrazic). Trebuie realizată o evaluare a informaţiilor pl, unite pentru a stabili, de exemplu, dacă acestea trebuie acceptate.i fiind veridice sau dacă trebuie considerate o tentativă de dezinformare din partea adversarilor12.

Adesea poate fi dificilă obţinerea directă a informaţiilor secrete în levante. În consecinţă, singura alternativă este încercarea de a deduce respectivele informaţii pornind de la datele disponibile, cum h li informaţiile pe care adversarii nu le consideră sensibile şi, de.h cea, nu păstrează secretul asupra lor.

De exemplu, cel mai direct şi mai credibil avertisment privind iminenţa unui atac ar putea proveni de la un agent infiltrat în cartierul general al inamicului. În absenţa unui astfel de agent, trebuie deduse intenţiile inamicului din diferite frânturi de informaţii referitoare la desfăşurarea trupelor acestuia, pregătirea lor pentru luptă nun nu 4* Uzarea rezerviştilor. În plus, informaţiile din surse publice pot fi (*m* asemenea, utile; de exemplu, înainte de atacul de la Pearl HaH$ Statele Unite erau interesate de locaţiile şi itinerariile vaselor ett Mfif ciale japoneze, considerând că, dacă japonezii ar fi intenţional intre în război, ar fi luat măsuri în vederea

retragerii flotei comei t late japoneze în ape sigure.

Până în acest punct, adepţii viziunii tradiţionale nu vor coillnti necesitatea unor astfel de acţiuni, în ciuda faptului că viziunea Mi asupra activităţii de informaţii pune accentul, în primul rând, *ţş* datele secrete. Apar semne de întrebare atunci când sfera activlliH de informaţii se extinde la nivelul „noii discipline a analizei Inimmaţiilor" promovată de Colby, o ştiinţă socială universală şi anticipativi care acoperă toate aspectele vieţii sociale.

Pentru o gestionare eficientă a problematicii militare şi a pol hm» externe, reprezentaţii unui guvern trebuie să dispună de mai nullit date despre potenţialii lor adversari, şi nu doar de informaţii socrfttţ de natură militară şi diplomatică. De asemenea, trebuie lunii Nl considerare şi alţi factori, cum ar fi situaţia economică a potenţialului adversar, tendinţele demografice, forţele politice interne. Refort UJJ la aceşti factori, dificultatea nu constă atât în culegerea dateliH neprelucrate (deşi aceste aspecte pot constitui o provocare, în ea/al unei societăţi închise, cu un sistem politic totalitar), cât în evaluării lor corectă.

De exemplu, în pofida caracterului deschis al procesului polltij american, unui observator american sau de altă naţionalitate i-ar fţ greu să înţeleagă şi cu atât mai mult să anticipeze deznodământul unei eveniment politic major, cum ar fi rezultatul unui vot în Congru sau alegerile prezidenţiale. În mod cert, pentru o coordonare

eficient! a politicii externe faţă de Statele Unite, o ţară trebuie să fie conştienţi de faptul că o bună înţelegere a acestor aspecte poate fi la fel de importantă ca şi obţinerea unor informaţii secrete privind securitatea naţională a Stateor Unite. Aşa cum a arătat Eliot Cohen, caracterul deschis al vieţii politice americane din anii ’30 nu a fost suficient pentru a le permite viitorilor adversari să o înţeleagă:

Deşi Statele Unite le erau accesibile agenţilor străini, atât celor oficiali, cât şi celor secreţi, într-un anumit sens, erau inaccesibile puteri h a mi, datorită incapacităţii acestora de a înţelege modul în i an hme tion* mi sistem democratic. Atât Germania, cât şi Japonia au Mihi în uimi în numărate rânduri sistemul politic american, tenacitatea,\ Iuvenil unaica acestuia, dar şi capacitatea sa de a se organiza, de a improviza l!«a produce rezultate. Aceste eşecuri majore pe linie de informaţii au «Ins la zdrobitoarea înfrângere a celor două state13.

Iu alte situaţii, informaţia care ar fi prezentat cel mai mare Mines pentru o naţiune nu putea fi considerată secretă deoarece, în rtMMiientul în care apărea necesitatea deţinerii acesteia, ea nici măcar nu exista încă. Sherman Kent exemplifică această situaţie prin problema a care s-a confruntat Uniunea Sovietică atunci când a încercat să miimeze dacă Statele Unite intenţionau să se împotrivească invadării» «acei de Sud de către Coreea de Nord, în 1950. Dacă agenţii, vieiici ar fi căutat în documentele americanilor dovezi privind Im i/ia acestora de a

se implica în conflict, nu ar fi găsit nimic, nitiucât preşedintele Truman a luat decizia respectivă după ce invazia i început: „Astfel, dacă intenţiile unei persoane pot fi anticipate i im citirea documentelor sale personale, iar strategia poate fi sta-initia pe baza informaţiilor aflate, situaţia de mai sus este un exemplu în care strategia e, prin definiţie, sortită eşecului” 14. Kent susţine că Milei de informaţii pot fi obţinute doar prin cercetare şi analiză:

Am arătat că, dacă există informaţii cu privire la situaţia strategică (termenul folosit de Kent pentru a se referi la capacitatea militară, politică şi economică a unei naţiuni de a acţiona pe scena internaţională) a statului Great Frusina (o mare putere ipotetică, în viziunea lui Kent), vulnerabilităţile acesteia şi modul în care sunt percepute, precum şi despre situaţia şi vulnerabilităţile altor state implicate, atunci există posibilitatea de a anticipa *acţiunile pe care le-ar putea întreprinde*. Pentru ca previziunile să fie cât mai reale, sunt necesare alte două categorii de informaţii. Mai întâi, trebuie cunoscute acţiunile pe care Great Frusina le-a întreprins în trecut. În al doilea rând, trebuie cunoscut, în măsura posibilului, modul în care Great Frusina îşi estimează propria situaţie în circumstanţele date15.

Nu e nicio îndoială că astfel de informaţii şi raţionamentele care» onduc la acestea constituie o parte vitală a gândirii strategice, în general, şi a politicii externe la nivel înalt, în particular. Nicio politică nu poate fi adoptată sau implementată

fără a lua în considerare potenţialele acţiuni ale altor state. Totuşi, nu este clar motivul j»…

care aceste activităţi trebuie considerate „activităţi de inimi…! secrete” şi trebuie să se desfăşoare în cadrul agenţiilor de informaţii 1 Această problemă, care ridică întrebări importante privind releţM dintre activitatea de informaţii şi factorii de decizie, a foii» – analizată în capitolul anterior.

Există două consecinţe ale viziunii netradiţionale asupra activtliţM de informaţii; totodată, trebuie remarcat accentul pe care acea»!! viziune îl pune pe activitatea de analiză a informaţiilor. Pun., consecinţă este că, în mare parte, analiza strategică poate şi trebuie să se desfăşoare în cadrul agenţiilor de informaţii. Această activllati în agenţiile de informaţii, este realizată conform unei metode yllln ţifice. Cu alte cuvinte, ştiinţele sociale pot sau ar trebui să furni/, ce, în scopul cercetării, metode care să aibă atributele cerecilitl ştiinţifice. Conform acestei viziuni, pot fi obţinute rezultate mal bune în activitatea de informaţii, chiar dacă acestea nu refleitl neapărat date obţinute prin mijloace secrete, ci previziuni bazate fapte cunoscute de factorii de decizie. Astfel, este posibilă utilizam informaţiilor secrete pentru evaluarea corectitudinii strategiilor17

O a doua consecinţă este că analiza informaţiilor poate fi separai! de procesul decizional, putând fi apolitică18. Ca urmare, s-a vorbit despre crearea, în cadrul comunităţii de informaţii, a unui depat tament analitic similar

unui grup de reflecţie performant 19. Din aceil punct de vedere, activitatea de informaţii constituie, într-o mai mici măsură, un element de sprijin direct pentru factorii de decizie, reprezentând mai degrabă un fel de „enciclopedie” sau serviciu de documentare, de ale cărui informaţii ar trebui să beneficieze nu numai adversarii politici ai factorilor de decizie, ci şi opinia publici internă şi internaţională20. De exemplu, Colby anticipează o eră a liberului schimb în lumea informaţiilor, în care naţiunile recunoat „avantajele reciproce ale schimbului de informaţii, respectiv faptul că ambele părţi pot beneficia de pe urma angajamentelor de a nu ascunde faptul că deţin armament şi de a nu obstrucţiona mijloacele tehnice de verificare ale altor state, conform acordurilor privitul controlul armelor” 21.

Oricât de neobişnuit poate părea acest lucru, potrivit acestei concepţii, activitatea de informaţii reprezintă un demers similar ştiinţelor sociale sau chiar echivalentul acestora.

Spionajul şi culegerea informaţiilor din surse tehnice

Indiferent de importanţa analizei în activitatea de informaţii, ca să fie analizate, datele brute trebuie să fie obţinute prin anumite mijloace, heşi unele pot fi obţinute din surse deschise (presă, radio, televi/iune), problema este că unele naţiuni nu fac publice nici măcar aspecte generale legate de forţele lor militare sau resursele economice alocate acestora. De aceea, chiar dacă viziunea lui Kent privind importanţa

relativă a surselor deschise şi secrete ar fi reală în cazul majorităţii statelor, este clar că nu e valabilă în cazul statelor care ascund aproape toate datele referitoare la structura forţelor sale militare.

În special după cel de-al Doilea Război Mondial, măsurile stricte de securitate întreprinse de fosta Uniune Sovietică au îngreunat activitatea de spionaj a Statelor Unite şi a ţărilor occidentale menită să conducă la obţinerea datelor necunoscute despre forţele militare sovietice. Aşa cum am menţionat deja, problema s-a rezolvat în special datorită dezvoltării unor tehnologii sofisticate de survolare a teritoriului sovietic – mai întâi avioanele U2, iar ulterior sateliţii de iccunoaştere.

Aceste mijloace tehnice au reuşit să învingă măsurile de securitate sovietice şi, în acelaşi timp, au eliminat, se pare, alte riscuri specifice activităţii de spionaj. Problema deteraiinării veridicităţii informaţiilor obţinute din surse umane a fost evitată prin utilizarea unor echipamente care nu pot induce în eroare şi nu pot fi corupte. În acelaşi litnp, accesul la o locaţie anume putea fi asigurat (deşi, pentru a realiza fotografii clare, condiţiile meteo sunt vitale). Şi din acest punct de vedere, informaţiile obţinute prin mijloace tehnice (*ţechini*) par mai credibile decât cele obţinute din surse umane (*humint*).

Ca urmare, după cel de-al Doilea Război Mondial, Statele Unite au acordat o importanţă exagerată informaţiilor *techint* în detrimentul informaţiilor *humint*. Acest lucru a făcut ca domeniul informaţiilor să fie considerat mai

degrabă ştiinţific, nu doar pentru că utiliza cele mai noi şi mai sofisticate tehnologii, ci şi pentru faptul că incertitudinile aferente utilizării surselor umane puteau fi eliminate în mare măsură prin recurgerea la surse tehnice, care ofereau o vastă acoperire a teritoriului inamic şi permiteau observarea dhetia evenimentelor. Rămâne de văzut dacă această dependenţă a Statelm Unite de sursele tehnice va continua în absenţa necesităţilor ib informare care au stat la baza acesteia22.

Subestimarea contraspionajului

O altă caracteristică a acestei noi concepţii este tendinţa de a subcallnia importanţa contraspionajului, în general, a dezinformării şi colinde* informării. Acest lucru este în strânsă legătură cu ideea conform căreia activitatea de informaţii reprezintă o variantă a ştiinţeltM sociale, ce are ca obiect analizarea altor ţări. Deşi activitatea da informaţii diferă, în anumite privinţe, de ştiinţele socială, cele dnuă discipline sunt similare, conform acestei viziuni.

De exemplu, Kent face observaţia că activitatea strategică de informaţii este, în terminologia propusă de el, o „extensie", în anumite sensuri, a efortului de cunoaştere, în general. Într-un anuiull sens, există „obstacole dificile ridicate special de către alte naţiuni" care creează impedimente. Cu toate acestea:

...oricât de importante ar fi, aceste extensii, aşa cum le-am denumit, *tiu au legătură directă* cu esenţa problemei: activitatea de informaţii *enW* acel simplu mod de a obţine informaţiile necesare

derulării unor acţiuni de succes. Informaţiile strategice sunt acele informaţii pe care se bazca/A relaţiile noastre externe, pe timp de pace sau de război23.

În schimb, din perspectiva „tradiţională”, faptul că un adversar încearcă să păstreze confidenţialitatea unor informaţii vitale este chiar esenţa problemei: dacă adversarii nu încearcă să-şi ascundă intenţiile, atunci efectuarea unor analize complexe nu se impune.

Aceste diverse puncte de vedere privind importanţa caracterului secret reflectă diferenţele de opinii cu privire la informaţiile secrete24. Dacă potrivit viziunii „tradiţionale” activitatea de informaţii este o componentă a confruntării propriu-zise cu adversarii, conform noii viziuni ea e, ca orice ştiinţă, un proces de descoperire a adevărului despre lume (natură), care poate fi denumit doar în mod metaforic luptă. Cu alte cuvinte, deşi natura are secrete, acestea nu sunt protejate în mod deliberat, sunt, pur şi simplu, adevăruri pe care nu le-am descoperit. Problema activităţii de informaţii nu constă atât în descoperirea intenţiilor secrete ale inamicului (după cum a de Miniistrat-o Războiul din Coreea, nici măcar adversarul nu poate şti «nu va reacţiona la viitoarele evenimente), cât în anticiparea compor-Minentului său, cu ajutorul metodelor ştiinţelor sociale. Acest lucru Mc valabil mai ales având în vedere faptul că analiza informaţiilor pune un accent tot mai mare pe evaluarea tendinţelor pe termen lung, arc au, adesea, un caracter social şi economic. În ceea ce

priveşte «niuaţia socială şi economică viitoare, nu pot fi obţinute informaţii lecrete, întrucât nici adversarul nu ştie cu certitudine ce se va întâmpla, ce alternative va avea la dispoziţie şi cu ce situaţii se va i onfrunta.

Această tendinţă de a afirma că activitatea de contrainformaţii ocupă un loc marginal are impact asupra importanţei acordate dezinformării şi combaterii dezinformării. Considerând că activitatea de informaţii este similară unui demers din domeniul ştiinţelor sociale, noua viziune, ignoră sau cel puţin minimalizează posibilitatea de/ în formării. Natura, deşi îşi poate ascunde secretele faţă de oamenii de»ninţă, nu încearcă, în realitate, să-i inducă în eroare.

Beneficiarii informaţiilor

(ele două viziuni asupra activităţii de informaţii diferă, de asemenea, în ceea ce priveşte beneficiarii şi utilizatorii datelor. Potrivit lui (olby, în concepţia tradiţională, şeful statutului este principalul şi, probabil, singurul beneficiar al informaţiilor. Această viziune se reflectă şi în Legea privind securitatea naţională din 1947, prin care a fost înfiinţată CIA, subordonată Consiliului Naţional de Securitate şi preşedintelui, şi nu Departamentului de Stat sau al Apărării. (onsecinţa acestui mod de organizare a fost, se pare, faptul că CIA avea să rămână în strânsă legătură cu factorii de decizie de la nivel înalt şi să monitorizeze şi coordoneze, în numele acestora, activitatea celorlalte agenţii de informaţii de la nivel departamental.

Întrucât noua viziune, susţinută de foştii

directori CIA Colby şi Turner, tinde să acorde o importanţă mai mică informaţiilor secrete, nu este surprinzător faptul că urmăreşte creşterea numărului de heneficiari ai datelor. De exemplu, Turner are în vedere înfiinţarea unei agenţii internaţionale de date obţinute prin satelit care să desfăşoare activităţi de culegere a informaţiilor prin mijloace tehnice, în numele ONU, şi să pună la dispoziţia întregii lumi aceste dale" I *h* asemenea, Colby consideră că suntem sau ar trebui să păşim Iuţi i» eră a liberului schimb de informaţii, în care volumul mare de indisponibile datorită tehnologiei moderne oferă beneficii reciph" nu unilaterale26. Această nouă eră trebuie să aibă la bază luuultf principii, care „trebuie să insiste asupra beneficiilor reciproce nit schimbului liber de informaţii".

Activitatea de informaţii şi problemele etica

Pdate părea ciudat să abordezi aspecte de ordin etic atunci căial discuţi un subiect ce vizează domeniul pragmatic al securităţii naţionale. Există riscul de a fi acuzat de naivitate. Totuşi, cei cute sunt preocupaţi de activitatea de informaţii s-au confruntat adesea cu problema moralităţii sale sau, mai precis, cu relaţia dificilă dinir aparenta imoralitate a demersurilor menite să-i convingă pe oameni să comită acte de trădare şi utilitatea sau chiar necesitatea acesim lucru27. În opinia lui Sun Tzu, în domeniul informaţiilor, cheia succesului o reprezintă capacitatea de a corupe persoane importante din tabăia inamicului. Sun Tzu apreciază că este vorba despre o problemă delicată, în special pentru cei care consideră că

loialitatea e o adevărată virtute. În opinia sa, „influenţa morală”, adică „acea influenţă care îi determină pe oameni să fie de acord cu opiniile conducătorilor lor”, este principalul element care determină victoria sau înfrângerea într-un război28. El pare însă conştient de faptul că necesitatea coruperii unor persoane de rang înalt şi a unor oameni de rând din alte ţări nu este în concordanţă cu idealul armoniei dintre supuşi şi conducătorii lor.

Chiar şi aşa, într-o manieră pe care o putem cataloga drept machiavelică, el îi îndeamnă pe cititorii săi să recurgă la spionaj, argumentând că varianta cealaltă – pe care, în opinia lui, cititorii ar considera-o mai „onorabilă” – este, de fapt, inumană. Având în vedere povara pe care o presupune un război şi efectul nimicitor asupra vieţii oamenilor, pe un ton hotărât, el atrage atenţia:

Cel care se luptă cu duşmanul său, de mulţi ani, pentru a obţine victoria într-o bătălie decisivă şi care, pentru că dispreţuieşte rangul, onorurile şi aurul, rămâne în necunoştinţă de cauză cu privire la situaţia inamicului mr complet dezumanizat. Un astfel de om nu este general, nu îl a da iţii i un folos suveranului său, nu are şanse de izbândi29.

I, ip (ul că Sun Tzu utilizează un argument de ordin etic, yl nu unul oi din practic în favoarea spionajului arată că el consideră neeoaar «îi determine pe cititori să îşi învingă scrupulele faţă de această

MII ludă.

În pofida perioadei din care datează acest exemplu, problema

…editaţii nu trebuie să fie privită ca o simplă curiozitate, având usecinţe de ordin practic în epoca modernă. De exemplu, în 1929. În iclarul de stat Henry L. Stimson, la scurt timp după ce a fost Mânuit în funcţie de preşedintele Hoover, a desfiinţat „Camera Neagră”, biroul criptografic al Departamentului de Stat, care timp. Îi peste un deceniu a deschis corespondenţa diplomatică şi alte mesaje codificate. Se spune că gestul său a fost motivat de faptul ci un gentleman nu citeşte corespondenţa altcuiva” 30. Din punctul de vedere al succesului repurtat de SUA în cel de-al Doilea Ră/.bol Mondial, menţinerea facilităţilor criptografice în cadrul armatei şi al marinei militare a fost un lucru bun, care a deschis calea obţinerii unor victorii importante în timpul războiului, în urma spargerii iodurilor diplomaţiei şi marinei japoneze.

Problema moralităţii activităţii de informaţii constă în faptul că aceasta e o formă clandestină şi duplicitară de luptă între naţiuni, spre deosebire de lupta armată, care este considerată, în mod tradiţional, o confruntare mai deschisă (şi, prin urmare, mai onorabilă). Activitate de informaţii implică, în esenţă, dezinformarea şi depinde în mare măsură de influenţarea unor cetăţeni ai statelor inamice să comită acte de trădare. Aşa cum reiese din exemplul lui Stimson, acest gen de activitate nu corespunde optimismului manifestat de americani cu privire la moralitatea de care trebuie să dea dovada relaţiile

internaţionale. (Faptul că informaţiile obţinute prin interceptarea comunicaţiilor sunt considerate în prezent „curate”, în comparaţie cu „imoralitatea” activităţii de spionaj, demonstrează măsura în care s-au diminuat standardele de moralitate aplicate la nivel internaţional) 31.

Viziunea lui Stimson şi-a pierdut valabilitatea în climatul politic instabil existent pe plan internaţional în anii ’30, ca să nu mai vorbim de cel de-al Doilea Război Mondial. Cu toate acestea, noua viziune asupra activităţii de informaţii, aşa cum a fost prezentata urni sus, are multe caracteristici care, în opinia susţinătorilor săi, o nu îl pară mai morală decât cea „tradiţională”:

Importanţa analizei (înţeleasă ca o ştiinţă şi având, astfel, prestigiul acesteia), în comparaţie cu activitatea de spionaj; primatul informaţiilor „curate” obţinute din surse tehnice asupra spionajului „imoral”; reducerea importanţei activităţii de contrainformaţii şi de/.tii formare, ceea ce atenuează percepţia negativă potrivit căreia activitatea de informaţii implică o confruntare între naţiuni; extinderea activităţii de informaţii spre alte domenii (schimbări sociale, evoluţii demografice, traficul de droguri etc.) mai îndepărtate de esenţa politică şi militară a confruntării dintre naţiuni; diversificarea beneficiarilor informaţiilor, tendinţa care transformi o componentă secundară a sistemului politic (care este utilizat! pentru promovarea intereselor naţionale, adesea în detrimentul altor state) într-un furnizor neutru de informaţii pentru guvern, opoziţie şi, în cele din urmă, pentru opinia

publică naţională f I internaţională.

Prin urmare, această nouă concepţie asupra activităţii de informaţii poate fi înţeleasă ca o reafirmare a viziunii optimiste a Statelor Unite după realităţile dure ale relaţiilor internaţionale din timpul celui de-al Doilea Război Mondial şi din primii ani ai Războiului Rece.

Capitolul 8

Elemente pentru o teorie a culegerii informaţiilor

Acest capitol reiterează întrebarea iniţială: ce sunt informaţiile? IV baza discuţiilor privind elementele de bază ale informaţiilor „h am ne situăm pe o poziţie superioară pentru a evalua diferitele «oncepţii actuale referitoare la informaţii, în special pe cele prezentate în capitolul anterior drept „noua concepţie americană" şi să încercăm să trasăm o definiţie generală.

Sintagma *activitate de informaţii* se utilizează cu referire la un «numit tip de date, la culegerea informaţiilor de acest tip (şi obstruc-lionarea activităţii similare a altora), la organizaţiile al căror rol este de a obţine (sau a nega) aceste date1. Din aceste trei categorii (informaţii, activitate şi organizaţie), prima este considerată de bază, în vreme ce următoarele două sunt definite prin termeni proprii. Astfel, prima problemă privind definirea informaţiilor este de a stabili destinaţia acestora.

Sherman Kent dă o definiţie pentru ceea ce el numeşte „informaţii externe pozitive la nivel înalt": adjectivele au rolul de a exclude

informaţiile care sunt de natură tactică sau operaţională (nu „la nivel malt”), informaţiile interne (nu „externe”) sau contrainformaţiile (nu „pozitive”). Conform opiniei lui Kent, „Cunoştinţele indispensabile pentru securitatea şi bunăstarea noastră nu sunt incluse. Sunt luate în discuţie atât informaţiile constructive cu care putem lucra pentru obţinerea păcii şi libertăţii pe mapamond, cât şi cele necesare apărării şi intereselor ţării noastre” 2.

În consecinţă, aceste informaţii sunt necesare în vederea derulării politicii externe şi luării hotărârilor majore privind evoluţia şi dispunerea forţelor militare pe timp de pace. Conform opiniei lut Kent, strategia de securitate naţională se poate baza pe informaţii

Chiar din titlul cărţii lui Kent (*Strategic Intelligence for Anw tU* în *World Policy*) rezultă că este vorba despre o dezbatere privim! serviciile americane de informaţii şi mai puţin privind domeniul îţi sine. Drept urmare, definiţia sa privind informaţiile este formulai! în conformitate cu cerinţele guvernului american. Totuşi, nimic din definiţia sau cartea sa nu pare să limiteze aplicabilitatea accalela numai la Statele Unite. Principiile de bază sunt de natură general! şi, într-adevăr, ţinând cont de ceea ce se doreşte să se afle despre o ţară străină, Kent nu vizează potenţialii adversari ai Americii, i inventează ţara „Great Frusina”, care serveşte drept ţintă general! a serviciilor de informaţii. În această abordare, eu consider că afirmaţiile lui Kent se aplică informaţiilor în general.

După cum a arătat Kent (prin utilizarea adjectivelor *la nivel înnli extern* şi *pozitiv*), definiţia pe care o dă tipurilor de informaţii nu este exhaustivă. Trebuie avut în vedere însă ceea ce el numeţile „informaţii tactice/operaţionale”, „informaţii interne” şi „contrainformaţii”. Cel mai important aspect este că descrierea lui Kent privind „informaţiile externe pozitive la nivel înalt” implică faptul că alte tipuri de informaţii nu sunt necesare pentru „securitatea l bunăstarea noastră”.

Se pare că definiţia lui Kent se concentrează numai asupra solicitării informaţiilor pe timp de pace. Pe timp de război, informaţiile ai trebui nu numai să ajute la luarea deciziilor militare de ordin stra tegic, ci şi la operaţiunile forţelor militare din teren. Totuşi, datele tactice/operaţionale ar trebui incluse în orice discuţie generală despre serviciile informaţii şi este greu de crezut că Kent nu va fi de acord

Situaţia poate fi diferită în ceea ce priveşte celelalte două restric ţii. Prima, limitarea informaţiilor la subiecţi externi pare arbitrară, cel puţin în teorie. Ameninţările la adresa ţării şi intereselor sale pot fi atât interne, cât şi externe sau pot implica grupări interne cu legături externe. După cum am văzut, definirea scopului informaţiilor interne reprezintă o sarcină extrem de dificilă.

Cu toate că, în general, vorbim despre securitate *naţională*, în aceste chestiuni un stat acţionează prin intermediul *guvernului* său, care de obicei consideră menţinerea formei de

guvernământ drept un interes primordial. Observaţi că, în definiţia de mai sus, Kent se it în.l la „apărarea Statelor Unite şi a *intereselor* lor”. Acest enunţ itemonstrează că democraţia americană ar putea fi pusă în pericol de teva care nu a constituit o ameninţare de natură fizică. Indiferent de muma datelor, informaţiile interne, necesare regimului pentru a ac jMoieja împotriva schimbărilor revoluţionare sau violente, trebuie,»le asemenea, să constituie o preocupare a serviciilor de informaţii. Desigur, subiecţii acestor informaţii şi importanţa conţinutului lor ilepind, în mare măsură, de natura guvernului (regimului).

În plus, apărarea unui stat poate depinde de obstrucţionarea atât în acţiunilor serviciilor secrete ale statului inamic, cât şi a operaţiunilor «le militare; contrainformaţiile, ca şi informaţiile pozitive, trebuie onsiderate necesare pentru „apărarea ţării”. Este mai puţin evident decât în exemplul anterior (informaţii tactice/operaţionale) faptul că Kent ar fi de acord cu completările noastre.

În orice caz, domeniul informaţiilor trebuie extins pentru a putea nu-lude şi aceste secţiuni. Dat fiind că serviciile oferă informaţiile necesare pentru derularea strategiei de securitate naţională, trebuie a aibă în vedere şi furnizarea unor date care să justifice utilizarea li aţelor militare pentru atingerea obiectivelor naţionale şi care să tontracareze activităţile de culegere a informaţiilor ale altor state, lotuşi, definiţia lui Kent privind informaţiile trebuie extinsă

semnificativ dacă este vorba despre „informaţii indispensabile pentru securitatea şi bunăstarea unui stat”.

Cu toate acestea, deşi trebuie să completăm definiţia lui Kent, ulăugând informaţiile relevante pentru derularea strategiei de secui flata naţională, în alte privinţe, definiţia este deja prea amplă. Un număr mare de informaţii (de exemplu, informaţiile tehnice din domeniul fizicii şi ingineriei) pot fi necesare pentru luarea deciziilor în ivind anumite aspecte legate de dezvoltarea tehnologiilor militare, însă aceste informaţii, în mod obişnuit, nu vor putea fi considerate secrete. În mod similar, se impune o înţelegere generală a fenomenelor meteorologice în planificarea acţiunilor militare, dar acest up de informaţii nu poate fi considerat de natură secretă3. Cu alte cuvinte, faptul că o anumită ramură a ştiinţelor naturii contribuie în mod semnificativ la îndeplinirea obiectivelor de securitate nu încamnă că aceste informaţii dobândesc automat caracter secret.

Situaţia este mai puţin clară când vine vorba despre ştiinţele, sociale. Activitatea de analiză specifică informaţiilor (de exemplu, situaţia politică dintr-o ţară străină şi prognosticul privind evoluţii acesteia) poate fi similară practicilor de evaluare din domenii) ştiinţelor sociale. Chiar şi aşa, cele două tipuri de analiză presimt importante deosebiri care sugerează că pot fi necesare abordlH diferite, deşi conţinutul este acelaşi.

Pentru a fi utilă, în evaluarea factorilor

determinanţi ai contentului politici dintr-o ţară străină, analiza informaţiilor trebuie «1 mi denţieze acele elemente care pot fi manipulate sau schimbate; mv obicei, beneficiarul analizei este interesat, în cele din urmă, influenţeze acea situaţie politică, nu numai să o cunoască, lie asemenea, o analiză ştiinţifică are ca scop să descopere cauzele fundamentale ale unei anumite situaţii, chiar dacă sau, mai,*U* dacă sunt acestea nu pot fi schimbate. În măsura în care ştiinţele sociale pot anticipa desfăşurarea evenimentelor (conform lui Kent, acesta fiind motivul pentru care sunt utile în domeniul informaţiiloi) acestea trebuie să considere viitorul deja prestabilit4.

Totuşi, relaţia dintre activitatea de informaţii şi ştiinţele sociale este complexă. Natura acestei relaţii se poate aborda mai bine în contextul altei diferenţe majore dintre activitatea de informaţii l ştiinţe – relaţia strânsă dintre informaţii şi natura lor secretă, pe de o parte, şi ştiinţa şi schimbul de idei, pe de altă parte.

Din punctul de vedere al viziunii tradiţionale asupra informatului (să nu menţionăm percepţia populară asupra acestora), ceea ce lipseşte din definiţia informaţiilor este elementul care îi conicii caracterul secret. Pentru Kent, într-adevăr, preocuparea pentru caracterul secret al informaţiilor nu reprezintă o parte inerentă a acestora, deşi el observă că un inamic poate încerca să blocheze accesul altcuiva la informaţiile pe care le solicită, el consideră că acel aspect este mai puţin important, asemănător problemelor organizatorice inerente structurii complexe a

serviciilor secrete moderne:

Indiferent de cât de importante sunt, aceste elemente complementare, după cum le-am numit (subtilitate, expertiză, *clandestinitate* şi mărime), sunt colaterale miezului problemei: activitatea de informaţii rămâne efortul cel mai simplu şi mai natural de a culege acele date pe care se bazează derularea cu succes a unei acţiunia.

Totuşi, legătura dintre informaţii şi caracterul secret este important;! pentru majoritatea acelora care fac distincţia între activitatea de minunaţii şi alte activităţi intelectuale. Reducând importanţa acestuia. Kent îşi menţine poziţia conform căreia nu există o diferenţă şif inentară între activitatea de informaţii şi ştiinţele sociale; articolul lui (olby analizat mai devreme a condus la concluzia că, pe viitor, „Clubul de la Roma", va deveni un model pentru serviciile de ml în maţii6.

I.egătura dintre informaţii şi caracterul secret reflectă problema fundamentală a relaţiei dintre activitatea de informaţii şi ştiinţă. Indiferent de similitudinile ce ar putea apărea, există o diferenţă Hementară a obiectivelor celor două propuneri. Scopul ştiinţei îl.«instituie cunoaşterea, fie de dragul ştiinţei, fie pentru cunoaşterea îi mai aprofundată a naturii – abilitatea de a manipula forţele naturale hmlorm voinţei omului în vederea obţinerii confortului, sănătăţii, longevităţii ş.a.m.d. Totuşi, conceptul privind lupta cu natura este numai o metaforă. De fapt, natura, deşi uneori este complicată şi dificil de înţeles, e indiferentă la eforturile umane şi nu acţionează iMcmeditat ca să le obstrucţioneze.

De asemenea, informaţiile implică o luptă reală cu inamicii tunului, dusă pentru a câştiga unele avantaje în defavoarea altora. Pun urmare, nu este nici surprinzător şi nici lipsit de importanţă faptul că aceşti inamici adesea încearcă nu numai să împiedice i lorturile cuiva de a-i cunoaşte, ci şi să dezinformeze şi să înşele. I secul informaţional al unei părţi poate fi succesul contrainformativ al celeilalte. Prin contrast, un succes informaţional al unei ţări nprezintă eşecul contrainformativ sau de securitate al inamicului acesteia.

Odată ce am înţeles că domeniul informaţiilor reprezintă o luptă mire două ţări, înţelegem de ce contrainformaţiile nu constituie un dement adiţional, ci parte integrantă a acestuia. Nu este suficientă limitarea sau distorsionarea a ceea ce adversarul poate afla, ci şi verificarea informaţiile culese despre un adversar fără ca el, prin resursele sale contrainformative, să detecteze acest lucru.

O obiecţie adusă acestei abordări este că ea ignoră rolul important pe care informaţiile din surse deschise îl pot juca în procesul culegerii de date. Totuşi, această obiecţie se bazează pe o neînţelegere. Informaţiile obţinute din surse deschise sunt vitale atât pentru activitatea de informaţii, cât şi pentru ştiinţele sociale; potrivit viziunii tradiţionale asupra informaţiilor, sursele deschise reprezintă în primul rând o modalitate de a depăşi barierele care blochează accesul du* i I* informaţiile căutate7.

Culegerea informaţiilor se bazează pe

obţinerea auriului *k* datele pe care cealaltă parte încearcă să le ascundă. CuligfH informaţiilor, în mod direct, înseamnă încălcarea barierelor de tttOUffH pe care cealaltă parte le-a instituit pentru a-şi proteja datelf «M interceptarea comunicaţiilor, sustragerea unor documente, sui votaţii zonelor restricţionate şi fotografiere, mituirea oficialilor cate îl acces la informaţii sau prin alte mijloace. Însă, în lipsa acceiuM direct la informaţii, este posibil ca acestea să fie deduse prin analr altor date – obţinute prin accesarea unor surse deschise, precum l altor date secrete.

În contextul acestei dezbateri, diferenţa dintre concepţia lui KeM despre informaţii şi viziunea care pune accent pe caracterul mh iü este, în principal, o chestiune de percepţie. Cea de-a doua concepţii subliniază faptul că inamicul îşi protejează informaţiile secrete!» timp ce Kent subliniază utilitatea datelor obţinute din surse deschlM într-o anumită măsură, preocuparea lui Kent pentru sursele dese Ihm, reflectă opinia sa conform căreia sursele secrete nu sunt mereu *éê* încredere. Este posibil ca un agent inamic să fie în realitate un agent dublu care dezinformează; poate este un impostor cu imaginata (care îşi atribuie o falsă calitate) şi care este suficient de inteligent ei să falsifice planuri de război verosimile pe care să le vândă la preţuri mari; este posibil că agentul să nu fie agent dublu, dar să fie deja compromis, astfel încât inamicul îl va aresta chiar în momentul în care transmite un mesaj important.

Deşi aceste fapte sunt adevărate, datele

obţinute din surse deschlue pot fi manipulate cu scopul de a dezinforma. Să luăm ca exemplu măsurile de dezinformare practicate de arabi, cu scopul de al convinge pe israelieni că nu va avea loc un atac în toamna anului 1973. Ei „au trecut de la salutarea iniţiativelor de pace ale lui domnului Kissinger din septembrie 1973 la înserarea într-un ziar libanez a unor ştiri referitoare la abandonarea şi deteriorarea echipamentelor militare din zona Canalului Suez” 8. Ideea este că orice tip de informaţii secrete pot deveni instrumente de dezinformare, iar analiza lor trebuie să ia în considerare acest aspect. Într-adevăr, aceasta este diferenţa esenţială dintre analiza informaţiilor secrete şi ştiinţele sociale: nu se falsifică rezultatele alegerilor cu scopul de

11 induce în eroare pe un sociolog care analizează a contonale U litava

* (tutca, desigur, să facă acest lucru cu alte inten (îi), Aualutul tif fcMitmtii nu este la fel de norocos. În cazul informaţiilor»ocrtM”, ar i «liiar cele obţinute din surse deschise nu sunt atât de inolonilvt pl*, uni par.

I) în acest motiv, era informaţională (în special volumul mare de Mi-am am din surse deschise aflate la dispoziţia factorilor de decizie)» «i afectează în mod substanţial această problemă. Deşi este important

* factorii decizionali să poată exploata eficient aceste surse de mii uniaţii, ele nu trebuie să devină canale suplimentare de dezina mare. Într-adevăr, se poate spune că, dat fiind faptul că factorii îi «i/.ionali s-au obişnuit să primească

informări la minut din sursele! ne fuse, a căror veridicitate nu este verificată, şi să obţină date lueet, nefiltrate de către analiştii a căror sarcină este să le evalueze în ansamblu, posibilitatea de a fi dezinformaţi este mare.

I) ieşi Kent subapreciază semnificaţia surselor secrete, aceasta ac im/cază pe considerente mai importante decât cele care stau la baza y i/lunii sale privind informaţiile obţinute din surse deschise. Spionajul»e limitează, în mod evident, la obţinerea informaţiilor pe care Inamicul le deţine deja; nu poate anticipa comportamentul inamicului atâta vreme cât acesta nu a luat încă o decizie şi, prin urmare, nu ştie ce acţiuni să întreprindă. În schimb, Kent consideră i, 1 această anticipare reprezintă este o sarcină informativă fezabilă, cu condiţia ca serviciile să aplice metodele folosite de ştiinţele sociale9.

După cum consideră Kent, această metodă este nu numai utilă reprezentanţilor statului, ci şi obligatorie – cine nu o aplică poate fi acuzat că se bazează pe globul de cristal sau pe intuiţie:

Atunci când beneficiarul ignoră evaluările serviciilor, bazându-se pe intuiţia sa, el ar trebui să înţeleagă că refuză utilizarea a doua instrumente pe care civilizaţia occidentală, începând de la Aristotel, le-a folosit pentru a-şi extinde orizontul cunoaşterii – instrumentele fiind raţiunea şi metoda ştiinţifică10.

Totuşi, indiferent cât de exact percepe situaţia politică un om de stat, se consideră ca fiind intuiţie, şi nu instrumente informaţionale, respectiv „raţionament şi metodă ştiinţifică”.

Dacă informaţiile ar putea în mod pertinent să conducă la pl. t tyuuteţ pe care le sugerează Kent în discursul său, factorii decizionali îl într-adevăr ridicoli să le ignore, iar sarcina lor ar fi mult mai uvol Optimismul lui Kent faţă de această abordare reflectă opiimuimrt general al ştiinţelor sociale din anii ’40 şi 50. Potrivii a* ***** concepţii optimiste, adoptarea unei metode ştiinţifice (precum versele metode cantitative) şi a unei perspective ştiinţifice (pe behaviorismul) vor permite ştiinţelor sociale o mai bună înţelege” I fenomenelor politice şi sociale (în cele din urmă şi cu acelaşi aueeetl în special, această percepţie va fi destul de exactă pentru a apilM funcţia de prognoză pe care Kent o atribuie informaţiilor.

În general, cercetarea în domeniul ştiinţelor sociale nu s-a materiali” în ultimele decenii, iar cercetătorii nu sunt foarte optimişti din aveţi punct de vedere. Capacitatea de anticipare a informaţiilor nu va avea impactul pe care şi l-a imaginat Kent. Acest fapt ridică o întreliait mult mai dificilă în legătură cu relaţia adecvată dintre activitatea de informaţii şi politică.

Toată lumea este de acord că activităţile de informaţiile se subof donează factorului politic, în sensul că sunt menite să serveam! factorilor de decizie (deşi, după cum s-a observat, această subordonau va fi luată în discuţie în măsura în care capacitatea de anticipare a informaţiilor care se bazează pe ştiinţele sociale ar putea fi pus! În practică). Anvergura acestui serviciu poate fi accentuată. Pe de cu parte, informaţiile sunt uneori folosite ca un serviciu de refer iuţi, sursă

de răspunsuri pentru anumite întrebări specifice". Pe de ulii parte, informaţiile pregătesc analize vaste a problemelor importante, completate cu prognoze. În ambele cazuri totuşi, informaţiile ajut! factorul politic care trebuie să ia deciziile.

Încrederea în aplicarea unei metode bazate pe ştiinţele sociale (dacă nu în prezent, atunci în viitorul apropiat) ce ar fi la fel de riguroasă şi avantajoasă precum metoda ştiinţifică în ceea ce priveşte lumea materială arată că, în mod firesc, experţii merită să ia în seamă subiectele cu care operează aceste metode. Totuşi, politica nu ar trebui să accepte numai informaţiile ca atare (dacă sunt disponibile fapte relevante, ar fi o nebunie să fie ignorate), ci şi evaluarea acestora.

Din păcate, o asemenea metodă bazată pe ştiinţele sociale nu există. În acest caz, evaluările informaţiilor ce încearcă să emită fitfiio/e (în special prognoze contingente) nu diferă de conduilllt r. me factorii decizionali le-ar putea trasa în situaţii similare, AII i.n i ar determina statusul relativ care să garanteze cele două mănări.

Analistul de informaţii probabil are o pregătire mai buna în iMneniu şi aproape cu siguranţă se pot aloca resurse considerabile

* mici activităţi (precum disponibilitate şi accesul la date). Factorul Hlhe probabil că ştie mai mult despre propriile politici de guvernare îi «lespre reacţiile diplomatice ale altor state faţă de acestea; este.«mii mai probabilă concentrarea asupra unor acţiuni fezabile pentru

* miluenţă situaţia. Cea mai cuprinzătoare şi

mai relevantă evaluare

* aluatiei din punct de vedere politic va rezulta din efortul comun al

* lor două grupuri.

Activitatea de informaţii are ca obiectiv culegerea unor date care»a servească naţiunea pe care o reprezintă în competiţia cu celelalte, hm urmare, aceasta are o natură dual㠹 indusă, pe de o parte, de faptul că se bazează pe informaţii, iar pe de altă parte, de faptul el sie o componentă importantă în cadrul conflictului dintre naţiuni i –.au cu alţi adversari, cum ar fi grupările teroriste transnaţionale ori, if, anizaţiile criminale). Prima componentă defineşte informaţiile «crete ca pe o ştiinţă socială cu caracter universal, care satisface nevoia de informare a factorilor politici despre alte ţări. În plus, asemenea noţiunilor ştiinţifice, informaţiile secrete de acest tip ar putea fi făcute publice, păstrându-şi totuşi caracterul secret.

A doua componentă, cea privind competiţia dintre naţiuni, ne i oiiduee în altă direcţie. Dat fiind faptul că informaţiile secrete devin un instrument al competiţiei, dificultatea de a le înţelegere nu se «latorează problemei în cauză; cele mai importante obstacole, reapectiv cele ce ar putea fi cele mai periculoase, sunt opera inamicului», are fie neagă informaţii, fie dezinformează în mod deliberat. Totuşi, nu contează ce informaţii se caută, trebuie să se ţină cont şi de serviciile secrete inamice; într-adevăr, aceste servicii devin principala pută a activităţii de informaţii întrucât capacitatea de a le penetra şi, în cel mai fericit caz, de a le manipula poate

avea un succes răsunător. Iu acest sens, informaţiile au o dinamică internă ce tinde să le transforme într-un duel al contrainformaţiilor, în care serviciul secret al fiecărei ţări, în majoritatea situaţiilor, caută să penetreze şi să manipuleze serviciul secret inamic.

În memoriile sale, fostul director CIA Colby critică modul. – care James J. Angleton, care a fost mult timp şeful contraspionajul" din CIA, a coordonat operaţiunile din departamentul său: „Înir udevfe se pare că acordăm o atenţie mai mare KGB ca inamic al CIA mm* Uniunii Sovietice ca inamic al Statelor Unite" 12. În mod evidettl, tg serviciu secret are menirea de a servi interesele naţiunii aale M contextul competiţiei dintre naţiuni. Însă, pentru a realiza acest luefuj de cele mai multe ori trebuie să se concentreze în special aauhi activităţii serviciilor secrete inamice.

Când un serviciu secret se axează în principal pe activităţii» serviciului secret inamic (şi pe posibilitatea ca serviciul inamic al fie implicat în operaţiuni de dezinformare), se expune riscului de I deveni „o imagine răsturnată" în care nimeni nu poate avea încredere şi nimic nu este ceea ce pare. Dacă serviciul pune constant la îndoiail veridicitatea tuturor dovezilor, nu poate ajunge la o mai bună tnţe legere a lumii exterioare. Activitatea de informaţii secrete este similail situaţiei în care fizicianul pune mai mult accent pe teorie decât le practică.

Dacă un serviciu de informaţii îşi ignoră inamicii, tot se expune riscului de a fi dezinformat şi de a percepe în mod eronat lumea care încearcă

să o cunoască. În probleme privind informaţiile secrete, analiştii cu greu pot avea încredere deplină în veridicitatea surselm pe baza cărora fac evaluări şi trebuie să aibă în vedere şi posibilitatea că acestea să fie eronate.

Aşadar, activitatea de informaţii are un caracter dual. Serviciile vor să afle tot ce se poate despre lume, iar obiectivul acestora poate fi caracterizat de versetul biblic pe care Allen Dulles, directorul CIA pe perioada mandatului preşedintelui Eisenhower, l-a adoptat ca motto: „Trebuie să cunoşti adevărul, iar adevărul te va elibera” 11 însă serviciile secrete nu trebuie să uite niciodată că aflarea adevărului implică o luptă cu un duşman care, la rândul lui, reacţionează – sau adevărul nu reprezintă un obiectiv, ci un instrument în obţinerea victoriei.

Note

Introducere

I Activitatea lui Sherman Kent, fost ofiţer de informaţii, a anticipat ai ni şi I şcoală de gândire de la sfârşitul anilor ’40 şi el rămâne cel mai cunoicut şi mai important reprezentant al acesteia. Subiectul a fost pentru puma dată expus în cartea sa *Strategic Intelligence for American World Pollty* (Princeton University Press, Princeton, NJ, 1949; reprim, 1%6) 9! este discutat în detaliu în capitolul 7 al acestei cărţi. Vezi şi hui au-a lui Bruce D. Berkowitz şi Allan E. Goodman *Strategic Intelligence for American National Security* (Princetonuniversity Press, Princeton, NJ, 1989), care, conform autorilor, se dorea a fi o carte „scrisă în acelaşi spirit” ca şi cea a lui Kent

(deşi nu este o variantă „actualizată” a acesteia). Autorii menţionaţi par să împărtăşească, parţial, cel puţin, concepţia lui Kent referitoare la informaţiile strategice, argumentând că, spre deosebire de serviciile operative, cele strategice au „o bază mai largă şi un obiectiv mai amplu, incluzând economia, politica, studiile sociale şi studiul tehnologiei. Serviciile de informare strategică sunt concepute să le ofere oficialilor o «perspectivă de ansamblu» şi prognoze pe termen lung de care au nevoie pentru a planifica operaţiunile viitoare” (pp. 4 – 5).

2. Senatorul David L. Boren, pe atunci preşedintele Select Committec on Intelligence, a precizat scopul reformelor propuse în domeniul serviciilor de informaţii de la începutul anilor ’90 pentru crearea unui „grup de experţi de talie mondială” – într-adevăr, „cel mai bun din lume”. „The Intelligence Community: How Crucial?”, *Foreign Affairs*, 71, nr. 3 (vara 1992), p. 61.

3. Una dintre primele şi cele mai cunoscute cărţi de acest tip începe cu următoarea afirmaţie: „În prezent, există în Statele Unite un cult puternic şi periculos – cultul serviciilor de informaţii”. Publicitatea este o armă vitală în lupta împotriva „acestei tagme secrete din ariston «pa politică americană”: „Obiectivul acestei lucrări este să le ofere vett ţenilor americani informaţiile interne de care au nevoie – şi la câte au dreptul, fără îndoială – ca să înţeleagă semnificaţia şi importanţa ai» «an probleme”. Victor Marchetti şi John D. Marks, *The CIA and the Cull Intelligence* (Knopf, New York, 1974), pp. 4, 12.

4. Publicaţia britanică *Intelligence and National Security* a manifestat un interes deosebit pentru acest subiect, publicând numeroase şi talii privind informaţiile secrete în cadrul „dimensiunii" istoriei militate l diplomatice.

5. Un exemplu elocvent îl constituie lucrările lui David Wise. Comparaţii de exemplu, două dintre primele sale lucrări (scrise împreună cu Thomai B. Ross) – *The Invisible Government* (Random House, New York, 1 %T) şi *The Espionage Establishment* (Random House, New York, 1967) – eu două volume mai recente, *The Spy Who Got Away*: *The Insight Story ttf Edward Lee Howard* (Random House, New York, 1988) şi *Mole Hunt The Secret Search for Traitors that Shattered the CIA* (Random Houie, New York, 1992). Titlurile în sine sugerează o schimbare de percepi în Cea mai recentă carte a sa, *Cassidy's Run*: *The Secret Spy War* ovei *Nerve Gas* (Random House, New York, 2000), se axează tot pe un cai de spionaj, o operaţiune cu un agent dublu care este posibil să fi avut urmări grave, neaşteptate.

6. Aceasta explică numărul mare al exemplelor privind al Doilea Război Mondial şi Războiul Rece; se cunosc mai multe aspecte legate de serviciile secrete din aceste perioade ale istoriei decât din alte perioade Trebuie accentuat totuşi că aspectele pe care le ilustrează aceste exemple sunt considerate de interes general; relevanţa acestora nu se limitea/fi la circumstanţele particulare ale acestor lupte.

7. O modalitate convenabilă de a fi la curent cu informaţiile accesibile publicului este vizitarea

diferitelor site-uri care conţin date privind servi căile secrete. Printre cele mai utile sunt site-urile aparţinând: Fédération of American Scientists (fas.org/irp), Muskingum Collège, Ohio(intellit, muskingum. edu/intellsite/maintoc.html), şi Loyola Collège, Maryland (www.loyola. edu/drept/politics/intel.html).

8. Trebuie menţionat că, înainte de a fi publicată, această lucrare a fost supusă analizei Central Intelligence Agency şi Select Committee on Intelligence din Senatul american. Aceste două organizaţii au convenit că *Războiul tăcut* nu conţine informaţii secrete.

Capitolul 1. Ce este activitatea de informaţii?

t Lucrarea lui Sherman Kent *Strategic Intelligence for Amrmon* HMH *Policy* (Princeton University Press, Princeton, NJ, 1949! rtf-tM ttiv este alcătuită conform acestei descrieri a serviciilor de luhuumtM În trei părţi.

Herbert E. Meyer, *Real-World Intelligence* (Weidenfeld and Nlat Hat HI, New York, 1987), p. 6. O scurtă bibliografie a lucrărilor de n pe lailtatt – informaţii de interes economic – poate fi găsită în lucrarea lui Multen David Steele *On Intelligence*: *Spies and Secrecy în an Opşn* Htif *M* (Armed Forces Communications and Electronics Association, l'alrftut. Va., 2000), pp. 375 – 378.

t Luaţi în considerare, de exemplu, eforturile depuse de administraţia americană în anii 1991 – 1992 de a alcătui o listă a „necesarului da informaţii" până în anul 2005. Impactul produs de încheierea Războiului Rece poate fi observat într-o mare varietate de subiecte ini-lu de pe lângă

necesităţile privind informaţiile tradiţionale (precum planurile nul urnişi intenţiile diplomatice ale ţărilor-cheie), lista conţinea solicitarea urau informaţii despre terorismul internaţional, proliferarea armelor de diatru-gere în masă, traficul de droguri şi o serie de probleme de naturii comercială şi economică. De asemenea, această listă cuprinde solicitările factorilor politici privind informaţii din domenii neconvenţionale precum noile tehnologii, demografia, migraţia populaţiei, problemele medicale şi de mediu. Vezi Loch K. Johnson, „Smart Intelligence", *Foreign Policy*, nr. 89 (iarna 1992 – 1993), pp. 60 – 61.

4. Pentru expunerea acestui subiect referitor la practica serviciilor secrete, vezi Adda Bozeman, *Strategic Intelligence and Statecraft*; *Selected Essays* (Brassey's [US], Washington, DC, 1992).

*». Dezvăluiri făcute în preajma prăbuşirii regimului comunist din Germania de Est ilustrează în mod izbitor ce poate însemna aceasta în practică. La momentul dizolvării sale, serviciul secret al Germaniei Democrate avea peste 85.000 de angajaţi, utiliza 500.000 de agenţi şi informatori part-time şi deţinea dosarele a şase milioane de cetăţeni est-germant, După cum a arătat Jefferson Adams, „pentru un stat cu o populaţie de aproximativ 17 milioane de persoane, a reprezentat o reţea internă de o capacitate extraordinară". Werner Stiller şi Jefferson Adams, „Preface to English Edition", în *Beyond the Wall*: *Memoirs of an East and West German Spy* (Brassey's [US], Washington, DC, 1992), pp, ix-x.

6. Cetăţenii unui stat democratic consideră că

acest lucru este evident, dar recunoaşterea faptului că cineva poate fi un opozant al guvernului din acel moment fără a fi inamicul unui regim sau al unei naţiuni repu im* o realizare valoroasă care nu trebuie pusă la îndoială. De anomehet conceptul de *opoziţie loială* implică posibilitatea unei opoziţii i tu» hm este. În vreme ce ia nivel teoretic este clar, la nivel practic demon «pite liberale întâmpină dificultăţi în a trasa o linie de demarcaţie. Prüm» a trecere în revistă a eforturilor guvernului american de a monitori" uneori de a distruge grupările şi organizaţiile considerate subveul vezi Richard E. Morgan, *Domestic Intelligence*: *Monitoring Disxtm* în *America* (University of Texas Press, Austin, 1980), pp. 15 – 87.

7. „The Attorney Genera Ps on General Crimes, Racketeering Enterpilie and Domestic Security Terrorism Investigations", 1983, partea a III Recomandările sunt republicate în US House of Reprezentatives, Commitle» on the Judiciary, *FBI Domestic Security Guidelines*: *Oversight Hearing* Congresul al 98-lea, prima şedinţă, 1983.

8. Pentru programul sovietic de achiziţii militare, vezi Katherine A *H* Siblez, „Soviet Industrial Espionage against American Military Technology and the US response, 1930 – 45", *Intelligence and National Security*, 14, nr. 2 (vara 1999), pp. 94 – 123, şi *Soviet Acquisition of Militarly Significmt Wzstern Technology*: *An Update* (Government Printing Office, Washington, DC, 1985). Pentru o scurtă prezentare a programului sovietic de înarmate din anii ’70 şi

reacţia Statelor Unite şi a ţărilor aliate faţă de acesta, ve/l Gus W. Weiss, „The Fairwell Dossier”, *Studies în Intelligence*, 39, ni *S* (1996), pp. 121 – 26, www.odci. gov/csi/studies/96 unclass/farewell, htin. Se pare că serviciul rus de informaţii externe a continuat să culeagă date secrete de natură tehnică şi industrială din alte ţări. Centrul american de contrainformaţii (The US Naţional Counterintelligence Center – NACK, organizaţie de colaborare între agenţii care operează sub auspiciile National Security Council) precizează: „Conform surselor media, preşedintele rus Boris Elţ în a confirmat la Moscova pe data de 7 februarie 1996 că Rusia este implicată în spionaj industrial, însă informaţiile culese de agenţiile secrete ruse nu sunt utilizate în mod eficient”. NACIC, *Counterintelligence News and Developments*; martie 1966, 1, www.nacic. gov/când/1996/mar96.htm. În ceea ce priveşte programul Chinei, vezi „Raportul Comisiei Cox”: *Report of the Select Committee un US* National Security *and Military Commercial Concems with the People’s Republic of China* (Government Printing Office, Washington, DC, 1999), capitolul 1, www.house. gov/coxreport.

9. Un fenomen separat, care nu vizează în mod direct problema sprijinului informaţional oferit factorului politic, îl constituie modul în care guvernul se foloseşte de informaţii pentru obţine bani. Un serviciu secret dispune de mai multe posibilităţi de a face bani, fie prin autofinanţare, fie prin nuanţare guvernamentală. Operaţiunile clandestine ale unui serviciu pot fi folosite pentru

a derula asemenea activităţi profitabile, precum îi alicul de droguri şi alte tipuri de contrabandă, iar în urma operaţiunilor t landestine se pot obţine informaţii din interior pentru speculaţii finanţa are. Nu este clar în ce măsură statele au folosit serviciile secrete în acest scop. Franţa reprezintă un astfel de exemplu care a devenit public, conform fostului şef al serviciului francez de informaţii externe, acest serviciu a aflat în noiembrie 1971 că guvernul american a decis să diminueze valoarea aurului în luna următoare, deşi acest lucru a depreciat semnificativ dolarul. „Prin vânzarea tacită a dolarilor şi cumpărarea francilor pe o serie de pieţe financiare internaţionale, Banca Centrală a Franţei a putut acumula un profit enorm – prin forţe proprii, suficient pentru a finanţa toate operaţiunile Serviciului.m Contele de Marenches şi David A. Andelman, *The Fourth World War* (Morrow, New York, 1992), pp. 114 – 115. io Datorită forţei lor tehnologice şi economice, Statele Unite s-au axat pe protejarea secretelor din aceste domenii. Din 1995, preşedintele a prezentat anual Congresului un raport privind spionajul extern care avea drept ţintă industria americană. Aceste rapoarte şi Legea spionajului economic din 1996 pot fi găsite pe site-ul Centrului naţional pentru contrainformaţii, www.nacic. gov. Alte surse includ General Accounting Office, *Economic Espionage*: *inform*ation *on Threat from US Allies* (GAO/T-NSIAD-96 – 114), www.nsi.org/Library/Espionage/allies, txt, şi Peter Schweizer, „The Growth of Economic Espionage:

America Is Target Number One", *Foreign Affairs*, 75, nr. 1 (ianuarie februarie 1996), pp. 9 – 14.

11. Restricţiile pe care şi le-au impus Statele Unite în ceea ce priveşte utilizarea informaţiilor de natură economică nu au pus capăt acuzaţiilor altor state, după cum este ilustrat de controversa din jurul, sistemului „Echelon" de culegere a datelor din comunicaţiile internaţionale. „I Schele»nu se referă la un sistem automat de selectare printr-o cantitate imenşii de date interceptate prin diferite metode de către Statele Unite *y* aliaţii acestora a căror limbă oficială este engleza. În februarie 2000, un raport oarecum fantezist pregătit pentru Parlamentul European acuaa Statele Unite şi pe aliaţii lor că au folosit informaţiile obţinute prin acest sistem pentru a-şi ajuta companiile să câştige avantaje comerciala. Dunum Campell, *Interception Capabilities 2000*, Raport către Directorul Of net al pentru Cercetare din Parlamentul European (Scientific and I» «lune al Options Assessment Programme Office), www.iptvreporu, mumillu Nu/ izreport, htm Report. Aceste acuzaţii au fost negate de ultra hiatul director al CIA, James Woolsey, într-o conferinţă de prell pentru data de

7 martie 2000. Woolsey a pretins că informaţiile care vizau corpoHMiţii străine erau limitate la trei domenii: aplicarea sancţiunilor, vitm echipamentelor militare şi a produselor utilizate în producerea mim*Im de distrugere în masă şi depistarea încercărilor de mituire cu» tl Mf corporaţiile neamericane aflate în competiţie cu cele americane. WUil a precizat că situaţiile

menţionate de Campbell se refereau la Inutrt Atiti corporaţiilor străine de a câştiga comenzile de export prin mim., oficialilor statului care făceau achiziţiile. Informare a Foreign I»im* Center, „Intelligence Gathering and Democracies: The Issue of Eeommtfe and Industrial Espionage", www.fpe. gov/wool0300.htm.

12. Conform unui studiu pe această temă, „Statele Unite deţin un"..«tehnic impresionant de monitorizare a unor arii întinse ale uscatului oceanelor şi atmosferei în scopuri legate de securitatea naţională. Ai tua* sisteme au cules date sofisticate care se întind pe zeci de ani yl t nu* constituie o arhivă istorică unică. De asemenea, aceste sisteme pul h utilizate pentru monitorizarea mediului". Scott Pace, Kevin M.O. CetntU Şi Beth E. Lachman, *Using Intelligence Data for Environmental Nerth Balancing Naţional Interests*, MI-799-CMS (RAND, Santa Monim. Calif., 1997), p. 2.

13. Pentru posibilele implicaţii ale erei informaţionale asupra servitul» secrete şi a agenţiilor de informaţii, vezi Bruce D. Berkowitz şi AII, în E. Goodman, *Best Truth*: *Intelligence in the Information Age* (YUIT» University Press, New Haven, Conn., 2000).

14. Comission on the Organization of the Government for the Conduct of Foreign Policy US (Comisia Murphy), *Report* (Government Printing Office, Washington, DC, 1975), p. 100.

15. Pentru analiza conflictelor de la sfârşitul anilor ’40 şi începutul anilor ’50 dintre Office of Policy coordination (agenţia guvernului american

pentru acţiuni secrete) şi Office of Special Operations (departamentul de spionaj al CIA), vezi John Ranelagh, *The Agency*: *The rise and Decline ofthi CIA* (Simon and Schuster, New York, 1986), pp. 199 – 200. Pentru informaţii privind rivalitatea dintre Secret Intelligence Service al Marii Britanii şi Speciale Operations Executive, care a fost înfiinţat, aşa cum spunea prim-ministrul Winston Churchill, pentru a „pune Europa pe jar" (adică derularea unor activităţi de sabotaj într-o Europă ocupată de nazişti în timpul celui de-al Doilea Război Mondial şi pentru susţinerea forţelor partizane care se opuneau ocupaţiei germane), vezi Cristopher Andrew, *Her Majesty's Secret Service*: *The Making of the British Intelligence Community* (Viking, New York, 1986), pp. 476 – 477.

1 ipitolul 2. Spioni, maşini şi biblioteci: culegerea informaţiilor i i Această clasificare cuprinde cele mai utilizate metode de culegere a informaţiilor, dar nu este completă. De exemplu, informaţiile secrete pot fi procurate şi prin furtul de documente sau coduri de la ambasada, ulversarului. Acest furt poate fi considerat *humint*, dar diferă de spionaj, aşa cum este el descris aici.

Din păcate, termenul *agent*, frecvent utilizat, este ambiguu: se referă în venerai la sursă, deşi uneori face trimitere mai degrabă la un ofiţer de informaţii, aşa cum se menţionează în lexiconul Federal Bureau of Investigations (FBI).

— Pentru a simplifica, această analiză se referă la ofiţeri de informaţii însărcinaţi cu spionarea ţărilor în care se află la post. Însă nu

este vorba despre asta, ofiţerii se pot afla la post în Freedonia pentru a recruta ruritani (din serviciile secrete străine, din serviciile de informaţii sau din instituţiile militare) care sunt şi ei aflaţi la post acolo. În acest caz, ofiţerii pot fi denunţaţi (apartenenţa lor la un serviciu de informaţi poate fi divulgată) autorităţilor freedoniene, scopul acoperirii lor fiind evitarea suspiciunile ruritanilor. De asemenea, ofiţerii de informaţii pot lucra în propria ţară pentru a recruta diplomaţii străini aflaţi acolo.

În alte dicţionare cu termeni din domeniu (cum este acelaul fontei Uniuni Sovietice), o deosebire comparabilă între ofiţerii „legali" şi cei „ilegali" ia locul acoperirii oficiale/acoperirii neoficiale (*nonofjhint cover* – NOC). Nu se face referire la legalitatea prezenţei ofiţerului în ţara-gazdă, ci la mijloacele prin care el comunică cu sediul»fiu centrul Un ofiţer ilegal este cel care comunică direct cu sediul său central, fRifl a menţine contactul cu instituţiile „legale" din ţara-gază* («mbe Mde, consulatul, camera de comerţ şi altele). În acest fel, un ofiţer Nllegal" seamănă cu un ofiţer aflat sub acoperire neoficială (NÖC), 5. În mod paradoxal, în unele cazuri, supravegherea pn-malului unei ambasade străine şi a străinilor în general de către «ervlolul Mitei «I unei ţări este atât de strictă încât singura modalitate siguri (te i ÜRHIHlt a cu o sursă din guvernul acelei ţări este ca un ofiţer de InrYirmuţil etile lucrează sub acoperire diplomatică să-l contacteze într-o maniei «ffiftttv „deschisă". De exemplu, în cazul lui Oleg Penkovnky, INIM umei în serviciul secret al

armatei sovietice (GRU) care a lucrul pentru»et vu tilde informaţii americane şi britanice la începutul anilor H0 M ßfHNiemu importantă a operaţiunii a fost cum să fie contactat în Maüi Wi und, supravegherea serviciilor de contrainformaţii sovletlee le h-nn dificilă orice încercare de a-l întâlni sau a comunica cu el e landul! Una din soluţii a fost să se profite de faptul că întâlnirile cu dilata diplomaţi americani şi britanici făceau parte din rutina muftiii im Penkovsky în domeniul ştiinţei şi tehnologiei. Un ofiţer de informaţii M putea da drept un astfel de diplomat, urmând să folosească un «ei tlM»** recunoaştere prestabilit (cum ar fi un ac de cravată cu pietre rofil) pentru ca Penkovsky să-l recunoască. După ce identifica perioada *tk* contact în cursul unei activităţi diplomatice de rutină, lui Penkovife urma să i se spună: „Mergi la toaletă, să spunem, şi [diplomatul/ ofiţerul de informaţii] te urmează după cinci minute şi îţi preia meftaM Nu este necesar să aibă loc vreo discuţie personală sau altceva de aveet fel. [Astfel de întâlniri sunt]... sigure pentru că în două sau trei în Im în materialul se află în mâini sigure şi afacerea este încheiată. Nu m» necesar să călătoreşti... Aceasta este metoda cea mai sigură Dtă nefericire, alte metode mai puţin sigure erau folosite mai des l sugerat că acestea au contribuit la identificarea lui Penkovsky ca informau*, la arestarea şi executarea lui ulterioară. Vezi Jerrod L. Schecter l Peter S. Deriabin, *The Spy Who Saved the World* (Scribner, New York, 1992), pp. 98, 287 – 299, 314 – 315, 409 – 411.

6. Pentru ca această „căsuţă poştală” să funcţioneze, trebuie să se înţelcaal că, deşi acest lucru nu este recunoscut oficial, o ambasadă sau o instituţie diplomatică are angajaţi capabili să lucreze cu informaţii de o importanţi deosebită sau secrete din surse voluntare. Un exemplu al caracterului cvasipublic al acestui tip de activitate secretă este dat de Allen Dullen, fostul director al CIA. După câte spune Dulles, curând după ce a tuni trimis ca ofiţer de informaţii în Elveţia, în timpul celui de-al Doilea Război Mondial, un ziar elveţian important a publicat un articol în care îl descria ca trimisul special şi secret al preşedintelui Roosevelt. Dulie» comenta că, „neoficial, cineva ar fi putut crede că această publici iau nedorită ar fi putut să-mi pună piedici. Ce s-a întâmplat a fost exact invers… Ca rezultat [al articolului], reţeaua mea a adunat o mulţime de informatori, unii excentrici, e adevărat, dar şi unii extrem de valoroşi” Allen Dulles, *The Crafi of Intelligence* (Harper and Row, New York, 1963), p. 7.

Pentru o relatare despre unul dintre cei mai valoroşi agenţi pentru care Dulles a jucat rolul de „căsuţă poştală”, vezi nota 17.

7. Operaţiunea sub acoperire poartă diverse denumiri, de exemplu: „post” (în jargonul american) şi „rezidenţă”(*rezidentura* în jargonul sovietic şi rus).

8. Problemele care apar odată cu angajarea unor cetăţeni ai ţării-gazdă în ambasade sunt bine cunoscute. Scriind despre perioada în care a ocupat funcţia de ambasador al SUA la Sankt-

Petersburg, Rusia, la începutul h în lor 1830, James Buchanan remarca: „Suntem mereu înconjuraţi de uptoni mai mari sau mai mici. Nu prea poţi să angajezi un servitor care mi este agent secret al poliţiei”. *Mission to Russia* (Arno, New York, IW»), p. 339.

Pentru o descriere jurnalistică mai recentă a problemelor de securitate ridicate de folosirea excesivă a angajaţilor cetăţeni ai ţării-gazdă în ambasade, vezi Ronald Kessler, *Moscow Station*: *How the KGB Penetrated the American Embassy* (Scribner, New York, 1989).

u De exemplu, ocuparea ambasadei americane la Teheran în noiembrie I o79 (şi sechestrarea personalului ambasadei) părea că a sistat complet culegerea de informaţii din surse umane în Iran de către Statele Unite. (ànd a început planificarea acţiunii militare de salvare a ostaticilor, nu era „niciun agent american pe teren” şi CIA a fost forţată să înfăţreze un agent în Iran pentru a ajuta la culegerea informaţiilor necesare pentru a planifica acţiunea de salvare. Charlie A. Beckwith şi Donald Knox, *Delta Force*: *The US Counter-Terrorist Unit and the Iran Hostage Rescue Mission* (Harcourt Brace Jovanovich, New York, 1983), pp. 196 – 197, 220 – 221.

În Acoperirea poate fi şi o afacere iniţiată, deţinută şi condusă chiar de serviciul de informaţii, o astfel de organizaţie fiind cunoscută ca aparţinând serviciilor de informaţii (*proprietary*). O organizaţie de acest tip poate fi utilă pentru activităţi secrete, precum şi pentru a

le oferi acoperire ofiţerilor de informaţii. De exemplu, o afacere în domeniul transporturilor poate să faciliteze transportul clandestin de arme şi provizii pentru rebeli

11. La începutul anului 1941, Sorge a raportat că Germania intenţiona s-a încalce pactul de neagresiune cu Uniunea Sovietică şi să o atace tu iunie. Rapoartele sale privind intenţia lui Hitler de a inculca acordul l data precisă referitoare la începerea ofensivei germane au font Ignorate de Stalin. Dictatorul sovietic era aparent convins că acestoa 1 alle informaţii despre duplicitatea germanilor fuseseră fabricate de britaniel pentru a provoca o ruptură între Germania şi Uniunea Nov lei le-A t pentru a împinge Moscova într-o alianţă cu Londra. Se pare el lui Irl e considerat rapoartele lui Sorge asupra intenţiilor japoneze mal 11 ci lit NU», parţial deoarece corespundeau cu mesajele japoneze interceptau de sovietici. Pentru relatări despre viaţa şi activitatea lui Sorgi ei *ift\\ßl* de informaţii sovietic, vezi Gordon W. Prange, Donald e ioliulelM fi Katherine V. Dillon, *Target Tokio*: *The Story of the* Suff *HA*¥ JMfif (McGraw-Hill, New York, 1984)

12. Pentru relatări despre viaţa şi activitatea lui Cohen ca agent Iftrfttthttf, vezi Stanley A. Blumberg şi Gwinn Owens, *The Survival* Afflaf *f Intelligence from World War I to the Présent* (Putnam. New ttitlt lui pp. 208 – 224.

13. Această relatare se bazează pe cartea lui John Barron, *KGB ïbtfa* f ** *Hidden Hand* (Reader’s Digest, New York, 1983; Berkley, New Viiffe 1985), pp. 247 – 314.

14. Dintre membrii blocului sovietic, Germania de Est a fost în mod lei adepta plasării unor ofiţeri cu acoperire neoficială (NOC) (sau, }m «., a folosi termenul sovietic, „ilegali”) în Vest, în special în Germania Vest, ţinta ei principală. Folosirea ofiţerilor ilegali a fost parţial 11 «i – Germaniei de Est deoarece eşecul din prima parte a Războiului Ren a dobândi recunoaştere diplomatică însemna că aceasta nu avea aiulm…» şi consulate în multe din ţările necomuniste. Utilizarea ofiţerilor ilaaill a fost facilitată şi de faptul că Germania de Vest a încurajai attit imigrarea din Est. Conform declaraţiilor unui fost ofiţer de informait! est-german, între două şi trei mii de agenţi erau în post până la ştiu iiiul anilor ’50. Cel mai faimos a fost Guenther Guillaume, care s-a ml tiu e cu succes în elita politică vest-germană, devenind secretarul personal al cancelarului Willy Brandt. El a ocupat această funcţie între 19 oM f 1974, când a fost arestat. Cristopher Andrew şi Oleg Gordievsky, *The Inside Story* (în Harperlouins, New York, 1990; ediţia Harper Perenntol 1991), pp. 448 – 450. Pentru descrierea utilizării de către Germania du Est a ofiţerilor ilegali, din perspectiva unui fost ofiţer de informaţii est-german, vezi Werner Stiller şi Jefferson Adams, *Beyond the Wnll Memoirs of an East and West German Spy* (Brassey’s [US], Washington, DC, 1992), pp. 41 – 118 passim.

15. Pentru o trecere în revistă a activităţilor *humint* ale Chinei, vezi Nichula* Eftimiades, *Chinese Intelligence Operations* (Newcomb, Arlington, Va, 1998), capitolul 5, pp. 28 – 44.

Pentru programul Chinei vizând obţinerea de tehnologie performantă din SUA, vezi „Cox Committee Report” *Report of the Select Committee on US National Security and Militat’s Commercial Concems with the People*’s *Republic of China* (Government Printing Office, Washington, DC, 1999), capitolul 1, www.house, gov/ coxreport. Vezi şi „China’s High-Tech Espionage”, o recenzie în două părţi a volumului *Sources and Techniques of Obtaining* Naţional *Defetist Science and Technology Intelligence*, un „manual” chinez despre spionajul în Vest, la Naţional Counterintelligence Center [în continuare nunul NACIC], *Counterintelligence News and Developments* (iunie şi septembrie 2000), vol. 2 şi 3. Aceste evaluări pot fi găsitela www. nacic. gov. site-ul NACIC.

16. Totuşi, nu poate fi exclusă posibilitatea ca, după ce a fost abordată de un ofiţer de informaţii străin, sursa să raporteze încercarea de recrutare propriului guvern şi să fie instruită „să coopereze”.

17. Vezi Joseph E. Persico, *Piercing the Reich*: *The Penetration of Nazi Germany by American Secret Agents during World War* II (Viking, New York, 1979), pp. 62 – 72, 328.

m Aiàt Burgess, cât şi MacLean au lucrat pentru Ministerul de Externe, în timp ce Philby a intrat în serviciul de informaţii britanic (MI6) şi a ajuns y lui direcţiei de contrainformaţii şi ofiţerul de legătură din Washington i îi CIA ŞI FBI. Vezi Andrew Boyle, *The Fourân Man* (Dial, New York, 179) pentru informaţii privind reţeaua de spionaj

sovietică formată în I *»30 la Cambridge University. Vezi şi Robert Cecil, „The Cambridge (omintern”, în Cristopher Andrew şi David Dilks (eds.), *The Missing Dimension*: *Governments and Intelligence Communities in the Twentieh (entury* (University of Illinois Press, Urbana, 1984).

I’J Serviciul de Securitate al Apărării, Centrul de Studii de Securitate, *Recent Espionage Cases*: *1975 – 2999* (septembrie 1999), www.dss. mil/ uaining/pub, htm, conţine o descriere şi rezumate ale cazurilor recente. Theodore R. Sârbin, Ralph M. Carney şi Carson Eoyang analizează diversele motivaţii ale implicării în activitatea de spionaj în *Citizen Espionage*: *Studies în Trust and Betrayal* (Praeger, Westport, Conn., 1994).

Îl) David Wise, *The Spy Who Got Away*: *The Inside* Story *of Edward Lee*

*Howard* (Random House, New York, 1998)...1 Vezi Mary S. Lowell, *Cast No Shadow*: *The Life of the American Spy*

*Who Changea the Course of World War* II (Pantheon, New York, 1992)., 2. Pentru o descriere a afacerii Dejean, vezi John Barron, *KGB*: *The*

*Secret Work of Soviet Secret Agents* (Reader* s Digest, New York, 1974), pp. 114 – 140.

M. Allan Dulles, *The Craft of Intelligence* (Westriew, Boulder, Colo., 1985), p. 216.

m. Dacă spionul capturat refuză să coopereze, se poate ca serviciul de informaţii care l-a prins să acţioneze în numele lui, trimiţând mesaje din partea sa. O astfel de substituire poate funcţiona în situaţii cum este spionajul în timp de război pe teritoriu inamic, când nu este de

aşteptat ca sursa să se întâlnească faţă în faţă cu angajatorii săi.

*15*. Cristopher Andrew, *Her Majesty's Secret Service*: *The Making of thi British Intelligence Community* (Viking, New York, 1986), p. 488. Pentru o relatare privind *The Double Cross System* scrisă de cel care a coordonat acest sistem, vezi J.C. Masterman, *The Double Cross System* in the *War of 1939 to 1945* (Yale University Press, New Heaven, Conn, 1972).

26. Un manual de pregătire vechi şi totuşi interesant, conceput de serviciile de informaţii ale armatei sovietice, conţine lecţii despre comunicarea şi controlul surselor de informaţii din Statele Unite. Acesta a fost unul din materialele furnizate de Oleg Penkovsky, un ofiţer militar sovietic care a spionat pentru Statele Unite şi Marea Britanie la sfârşitul anilor '50 şi începutul anilor '60. „The Prikhodko Lecture" în Frank Gibeny i».» *The Penkovsky Papers*, (Doubleday, New York, 1965), pp. 102-IM

27. Wise, *The Spy Who Got Away*, pp. 198 – 205. Pentru ca trucul II Rf complet, la întoarcerea acasă, soţia lui Howard a sunat la biroul torului acestuia. La acea oră, era de aşteptat ca doctorul să nu fii l birou şi a răspuns robotul; soţia lui Howard, presupunând că ich Ihm».» era ascultat, a pus la telefon mesajul pe care Howard îl înregistrau mai devreme. Acest lucru urma să ajute FBI să confirme că Howard I a întors acasă cu soţia lui. Aşa cum s-a dovedit, eforturile familiei Howwa4 au fost inutile; în mod inexplicabil, agentul FBI care supraveghea (MMI nu a observat

că familia Howard plecase de acasă şi maşina lor nu a hm, de fapt, urmărită.

28. Un exemplu al interacţiunii dintre filaj şi contrafilaj este descrii *é*ş Peter Wright, un fost funcţionar MI5 (serviciul de contrainformaM britanic), în cartea sa *Spycatcher*. Wright spune că tehnicienii sovlettel care operau la ambasada din Londra puteau să monitorizeze comunicatllla echipelor mobile de filaj („Observatorii") folosite de MI5. Prin anal i/arta acestor comunicaţii şi corelarea lor cu propriile operaţiuni, sovieticii puteau deduce dacă o anumită întâlnire dintre un ofiţer de informaţii sovietic şi sursa lui era posibil să fie supravegheată. Dacă era supravegheau, ofiţerul era anunţat să anuleze întâlnirea. Serviciul britanic de conti am formaţii, conform celor scrise de Wright, a identificat această slăbiciuni a sistemului de supraveghere când a detectat emisii electronice din ambasada rusă care au fost asociate direct cu operaţiunile de interceptară radio ale comunicaţiilor Observatorilor. Pe scurt, aşa cum spune Wright, MI5 îi supraveghea pe sovieticii care îi supravegheau pe Observatori, care, la rândul lor, îi supravegheau pe sovietici. Wright, *Spycatcher The Candid Autobiography of a Senior Intelligence Officer* (Viking, New York, 1987), pp. 52 – 57, 91 – 93.

29. Pentru ilustrarea metodelor necesare realizării unei „căsuţe poştali) impersonale", vezi descrierea făcută de John Barron reţelei de spiona sovietice conduse de John Walker, *Breaking the Ring* (Houghton Mifflin, Boston, 1987), pp. 80 –

96.

30. Declaraţiile sub jurământ ale reprezentanţilor FBI în sprijinul mandatelor de arestare şi percheziţie în cazul Hanssen conţin citate ample din mesajele schimbate de el cu KGB şi cu agenţia rusă care i-a succedai KGB, Slujba Vneşnâi Razvedki (Serviciul de Informaţii Externe sau SVR). În aceste mesaje, Hanssen refuza întâlniri faţă în faţă (chiar şi în străinătate) din motive de securitate şi insista să fie folosite aproape în exclusivitate căsuţe poştale impersonale. (Contactul iniţial a fost stabilit prin poştă la reşedinţa unui ofiţer de informaţii sovietic; în câteva ocazii, s-a comunicat şi prin telefon.) Declaraţiile sub jurământ sunt

»Îisjxjnibilepe www.fas.org/iro/ops/ci/hanssen attidavit, htint, uit adev Aiet manual referitor la căsuţele poştale impersonale.

H Herbert Rommerstein şi Stanislav Levehenco, *The KGB* m/mm/ *Înß Main Enemy*": *How the Soviet Intelligence Service Opérâtes ttRUIML die United States* (Lexington, Lexington, Mass., 1989). p. 293. Noln inrmându-i pe ofiţerii sovietici aflaţi la post în Viena, KGB reducea astfel şi riscul ca supravegherea acestora de către SUA să compromită* operaţiunea Walker.

11 Nicholas Eftimiades, *Chinese Intelligence Operations* (Newcomb, Ari ington, Va., 1998), pp. 33, 36 – 37.

H La sfârşitul anului 1953, serviciul de informaţii sovietic, numit pe atunci MGB (Ministerul de Securitate a Statului), făcea parte din Ministerul de Interne (MVD); consolidarea

acestor două autorităţi importante a fost rezultatul unei acţiuni în forţă a fostului şef al serviciului de informaţii şi conspirator important la Kremlin, Lavrenti Beria, în urma morţii lui Stalin, în martie 1953. După arestarea şi executarea lui Beria, în decembrie 1953, serviciul de informaţii sovietic a fost din nou separat de Ministerul de Interne şi numit KGB (Comitetul de Securitate a Statului). Defectările au avut loc în aceste momente de schimbare în serviciul de informaţii. Cei cinci defectori (şi ţările în care au defectat) au fost: Iuri Rastvorov (Japonia); Piotr Deriabin (Austria); Vladimir şi Evdokia Petrova (Australia); Nikolai Khokhlov (Germania de Vest). Vezi Gordon Brook-Shepherd, *The Storm Birds*: *Soviet Fost-War Defectors* (Weidenfield and Nicholson, Londra, 1998), pp. 57 – 131.

14. Conform Stockholm International Peace Research Institute, „Fact Sheet: Iraq: The UNSCOM Expérience" (octombrie 1998), disponibilă pe editors, sipri, se/pubs/Factsheet/UNSCOM.pdf, importanţa celui mai mare centru de cercetare, dezvoltare şi producţie a armelor biologice din Irak, al-Hakam, nu a fost recunoscută până la defectarea lui Hussein al-Kamal, deşi inspectorii UNSCOM vizitaseră deja locaţia. În mod asemănător, după defectarea sa în 1994, un om de ştiinţă important implicat în programul nuclear din Irak a oferit primele informaţii detaliate despre istoria programului şi mecanismele interne de funcţionare a acestuia. Judith Miller şi James Risen, „Defector Describes Iraq's Atom Bomb

Push", *The New York Times*, 15 august 1998, p. Al.

35. Relatarea îi aparţine lui David C. Martin, *Wilderness of Minors* (Harper and Row, New York, 1980). Relatări mai recente despre aceste dezbateri din cadrul comunităţii de informaţii americane se găsesc în *Cold Warrior*: *James Jesus Angleton, the CIA's Master Spy Hunter* de Tom Mangold (Simon and Schuster, New York, 1991) şi *Deception*: *The Invisible War between the KGB and the CIA* de Edward J. Epstein (Simon and Schuster.

New York, 1989). Cărţile lui Mangold şi Epstein redau puncte il».1 clare, dar opuse, reflectând dificultatea de a trage o concluzie nu a-i buna-credinţă a unor defectori.

36. Chiar şi anterior, baloanele au fost folosite ca posturi de ohm nu* aeriene de către Prima Republică Franceză, în 1794, şi de către AimM Unionistă în Războiul Civil American. În niciunul din cazuri im, obţinut niciun succes notabil şi ambele armate şi-au abandonat luti târziu „forţele aeriene" în formare. Vezi William E. Burrowl, / «./ *Black*: *Space Espionage and National Security* (Random House, N» * York, 1987; Berkley, New York, 1988), pp. 26 – 28.

37. Andrew, *Her Majesty's Secret Service*, p. 133.

38. William Mitchell, *Memoirs of World War I*: *„From Start to Finhh uf Our Greatest War"* (Random House, New York, 1960), p. 59, citul la cartea lui Rüssel F. Weigley, *The American Way of War* (Indiana Univenll Press, Bioomington, 1977), p. 224.

39. O relatare profesionistă privind spionajul ştiinţific britanic în timpul celui de-al Doilea Război Mondial, scrisă de unul din experţii acestuiM o găsim în cartea *Most Secret War* de R.V. Jones (Hamish Hamilton, Londra, 1978), republicată în Statele Unite sub titlul *The Wizard Wni British Scientific Intelligence*: *1939 – 1945* (Coward, McAnn a-mi Geoghegan, New York, 1978).

40. John Prados, *The Soviet Estimate*: *US Intelligence Analysis and Russitm Military Strength* (Dial, New York, 1982), pp. 38 – 50.

41. Prados, *The Soviet Estimate*, pp. 29 – 30. Pentru o descriere mai detaliata, vezi Curtis Peebles, *The Moby Dick Project*: *Reconnaissance Balhorn over Russia* (Smithsonian, Washington, DC, 1991).

42. Stephen E. Ambrose, *Eisenhower*: *The President*, vol. 2 din *Eisenhowtt* (Simon and Schuster, New York, 1984), pp. 264 – 265.

43. Încă din 1946, corporaţia RAND, un grup de experţi având contract cu Forţele Aeriene ale Armatei de la vremea respectivă, a fost solicitata fi cerceteze fezabilitatea şi utilitatea sateliţilor pe orbita Pământului, tu studiul său, RAND a arătat că sateliţii pot, printre alte lucruri, îl servească drept „aeronavă de supraveghere care nu poate fi doborâtă tio un duşman ce nu deţine tehnici asemănătoare”. Pentru un rezumat al studiilor RAND, vezi Walter A. McDougall, *The Heavens and the Earth*: *A Political History of the Space Age* (Basic Books, New York, 1985), pp. 102 – 111. Pentru o descriere mai detaliată, vezi Merton *V.*

Davies şi William R. Harris, *RAND's Role in the Evolution of Balloon and Satellite Observation Systems and Related US Space Technology*, R-3692-RC (RAND, Santa Monica, Calif, septembrie 1988).

44. Ambrose, *Eisenhower*, vol. 2, p. 228.

«1 Referitor la decizia Statelor Unite de a construi un satelu de iih tute triftete, eşecurile de la început şi succesele programului, vezi McDougall, *în¥ llnivens and the Earth*, pp. 97 – 131, 190, 224, şi Dwaync A Day, Jnim M. Logsdon şi Brian Latell, *Eye in the Sky*: *The Story of tht* (cântfMJ, S/»v *Satellites* (Smithsonian, Washington, DC, 1998).

«fi Vezi declaraţia gen. – mr. B.L. Schriever, *Inquiry into Satellite and Missile l programs*, Audierile anterioare în faţa Subcomitetului de investigare privind starea de pregătire al Comisiei pentru serviciile armate din Senarul SUA, al 85-lea Congres, a doua sesiune, 6 – 22 ianuarie 1958, partea a II-a, 1633 – 1635.

1/ Deşi se poate presupune că sovieticii au înţeles că existau astfel de capacităţi de recunoaştere, nu s-a considerat oportună atragerea atenţiei publice asupra acestui fapt. La vremea respectivă, Uniunea Sovietică, neclintită în decizia de a respinge planul „Open Skies", a considerat că recunoaşterea din spaţiu reprezintă o activitate de spionaj şi contravine legilor internaţionale în aceeaşi măsură ca şi recunoaşterea aeriană. Din cauza acestei poziţii, guvernul Statelor Unite era îngrijorat că o dihcuţie deschisă privind recunoaşterea din spaţiu

va încuraja Moscova să o considere o problemă importantă. Aşadar, în ciuda discuţiilor publice despre recunoaşterea din spaţiu, la sfârşitul administraţiei Hinsenhowet, administraţia Kennedy, care nu vedea niciun motiv să-l stârnească f»e Hruşciov susţinând deschis dreptul Statelor Unite de a derula o astfel de recunoaştere, a luat „măsuri... pentru a trece programul de recunoaştere spaţială din zona gri în zona neagră" (Burrows, *Deep Black*. p. 107). Totuşi, aşa cum observă Walter McDougall, „până în 1963 bucuria [Guvernului Statelor Unite] a luat sfârşit... Sovieticii au început să lanseze propriii sateliţi de spionaj... [care, în cele din urmă, au legitimai supravegherea din spaţiu". *The Heavens and the Earth*, p. 348.

IX. Eric Schmitt, „Spy-Satellite Unit Faces a New Life în Daylight", *The New York Times*, 3 noiembrie 1992, p. A10.

l o în mod paradoxal, efectele de distorsiune generate de atmosfera terestră pot fi mai puţin problematice pentru fotografierea din spaţiu decât pentru cea aeriană. La începuturile fotografierii din spaţiu, faimosul expert în rachete Wernher von Braun observa că, „atunci când foto grafiezi... din spaţiu, interferenţele şi turbulenţele sunt departe. Atmosfera este mult mai transparentă de deasupra decât de dedesubt". Pentru a ilustra afirmaţia, a sugerat următoarea demonstraţie: „Luaţi o coală de hârtie cerată. Ţineţi-o aproape de faţă şi veţi vedea ceva vag. Ţineţi o pe o coală de ziar şi este perfect transparentă. O situaţie asemănătoare este şi aici". Discursul la a doua întâlnire anuală a

Asociaţiei Armatei SUA, 26 octombrie 1956, citat în McDougall, *The Heaven and the Earth*, p. 224.

50. Această explicaţie a unui circuit cu cuplaj de sarcină este prelUNtl ttht Harold Hough, *Satellite Surveillance* (Loompanics, Port Towiwmie Washington, DC, 1991), pp. 46 – 48.

51. Pentru că foloseşte lungimi de undă mari (comparativ cu lungim»* Al undă a luminii), radarul produce o imagine neclară, un simplu pur t luminos pe ecran. Modalitatea de a compensa lungimile de uihla mm mari este de a creşte dimensiunea antenei. Din acest motiv, IHM perfectată o tehnică numită radar cu apertură artificială (SAR), în t ** o antenă mică mişcându-se în linie dreaptă are efectul unei antene itiuM mai mari. Cu procesoare puternice la bord, sistemele SAR colecte”! îi coroborează mii de „imagini” cu rezoluţie scăzută pentru a form* în imagine mult mai coerentă. Pentru mai multe detalii privind funcţionate* sistemelor SAR, vezi Charles Elachi, „Radar Images of the Earth ftowt Space”, *Scientific American* (decembrie 1982), pp. 54 – 61.

52. US Departament of Defense, *Conduct of the Persian Gulf War*: *I* /,»…/ *Report to Congress* (US Government Printing Office, Washington, DC, 1992), p. 138, analizează tactica *tankplinking* care a fost dezvoltata ta timpul Războiului din Golf pentru a exploata acest fenomen. Un snlelii poate utiliza şi un scanner multispectral care ia imagini ale ţintei folo Nlmt frecvenţe multiple din interiorul şi din exteriorul spectrului de lumini vizibilă. O imagine multispectrală poate furniza informaţii despre luna care nu sunt detectabile cu

ochiul liber. În timpul Războiului din Golf, de exemplu, imagistica multispectrală a fost folosită pentru a identifica zone de mică adâncime în apropierea coastei, informaţii necesare pentru planificarea operaţiunilor cu amfibii. În plus, deoarece majoritate* imaginilor sunt acum formatate digital, datele pot fi manipulate mai uşor pentru a sublinia diferenţele mici, având ca rezultat un contrast mal mare şi, în consecinţă, o rezoluţie mai mare. Astfel, de exemplu, diferenţe topografice minore care nu pot fi detectate printr-o fotografie tradiţională sunt redate mai clar prin tehnicile de procesare avansate.

53. Conform Fédération of American Scientists's World Space Guide (www.fas.org/spp/guide/index.html), China derulează operaţiuni de fotorecunoaştere spaţială încă din 1975, iar Franţa din 1995. Planurile japoneze subliniază necesitatea lansării a patru sateliţi (doi optici şi doi cu radar cu apertură artificială), începând cu 2002.

54. Vernon Loeb, „US Is Relaxing Rules on Sale of Satellite Photos", *The Washington Post*, 16 decembrie 2000, p. A3.

55. Lista este preluată dintr-un studiu de caz pregătit pentru John F. Kennedy School of Government la Harvard University. Rachel E. Billingslea, Matthew R. Domsalla şi Brian C. Payne, *The National Reconnaissance Office*: *A Strategy for Addressing the Commercialization of Space Imagery*, 6 aprilie 1999, www.fas.org/eye/ADA366610.htm.

Răspândirea imagisticii comerciale prezintă şi

avantaje, şi dezavantaje. Pe de o parte, guvernul îşi poate satisface o parte din necesităţile în materie de imagistică prin achiziţionarea unor produse de la cei ce le comercializează, aceasta permiţând serviciilor de informaţii să se concentreze asupra necesităţilor speciale care nu pot fi acoperite de sectorul comercial. Pe de altă parte, proliferarea sateliţilor comerciali pentru lotorecunoaştere face dificilă sarcina unui guvern de a ascunde amplasările strategice de forţe şi operaţiuni. (Statele Unite au încercat să rezolve problema prin rezervarea dreptului de stopare a activităţii sateliţilor, cu referire la sistemele pe care le autorizează, pentru a împiedica operatorii să fotografieze anumite zone în perioade de criză, acest drept neextinzându-se însă şi asupra sistemelor operate de entităţi din afara Statelor Unite) Pentru o scurtă descriere a acestui subiect, vezi Naţional Commission for the Review of the National Reconnaissance Office, *Report* (noiembrie 2000), www.fas.org/irp/mo/commission.

v» Detectarea şi analiza radiaţiilor electromagnetice emanate din surse radioactive sau detonări nucleare nu sunt considerate componente de *elint*. Vezi, de exemplu, definiţia „informaţiilor secrete electronice” în *Dictionary of Military and Associated Terms* al Departamentului de Apărare, Statul Major Reunit al SUA, JCS Publication l-02 (Joint Staff, Washington, DC, 12 aprilie 2001), p. 144, www.duc. mil/doctrine/jel/ newspubs/jp 1 – 02. pdf.

*ŞI*. Aşadar, undele electromagnetice generate

de maşinile de scris electrice sau computere pot fi interceptate şi analizate; în acest fel, textele sau datele introduse pe aceste dispozitive pot fi recuperate. O modalitate de a evita acest pericol este ca dispozitivele de acest tip să fie ecranate pentru a reduce emanaţiile şi pentru a se împiedica încercările de interceptare. Un fenomen asemănător este emiterea involuntară a unor semnale electromagnetice printr-un cablu. În unele cazuri, s-a descoperit că dispozitivele destinate codificării mesajelor emit semnale slabe care conţin text necodificat. Conform declaraţiilor unui ofiţer de contrainformaţii britanic, comunicaţiile Ambasadei Franţei la Londra au fost vulnerabile deoarece francezii nu şi-au ecranat corect dispozitivele de procesare a informaţiilor, pentru a preveni astfel de emisii electronice involuntare. Ca rezultat, împreună cu textul codificat corect, cablul telex care ieşea din ambasadă transmitea şi „ecoul" electronic slab, dar distinct al mesajelor diplomatice, aşa cum fuseseră tastate iniţial. Dispozitivele de interceptare secrete instalate la mică distanţă de ambasada franceză le-au permis britanicilor să citească mesajele diplomatice necodificate ale aliaţilor lor. Peter Wright, *Spycatcher*, pp. 109 – 111.

58. Practica interceptării mesajelor antedatează folosirea radioului ca mijloc de comunicare; curierii erau prinşi şi scrisorile deschise înainte ca radioul să fi existat. În plus, comunicaţiile prin telegraf puteau în interceptate. În timpul Primului Război Mondial, britanicii au

avu, un avantaj în domeniul informaţiilor deoarece companiile lor delii unui fi operau multe din liniile internaţionale importante de comunicai!!

59. Tocmai pentru că mesajele radio pot fi uşor interceptate, moftiu»le importante sunt cel mai probabil trimise în formă criptată. Astfel, *amm* şi criptanaliza, descifrarea codurilor şi cifrurilor, sunt strâns legale, deşi criptanaliza ar trebui considerată probabil o metodă de anal l/S a informaţiilor (mai degrabă decât o metodă de culegere a informait Hui) şi din acest motiv este discutată în următorul capitol.

60. Datorită preocupărilor continue privind confidenţialitatea, este puilit probabil să se scrie în viitorul apropiat o lucrare exhaustivă doi pii utilitatea *comint* în timpul Războiului Rece. Cu toate acestea, istorii II de la Agenţia Naţională de Securitate (NSA, serviciul SIGINT al SUA) susţin că succesul americanilor în decodarea sistemelor sovietice de cifrare în anii ce au urmat celui de-al Doilea Război Mondial „a putut fi comparat cu succesele înregistrate în timpul celui de-al Doilea Ră/.bnt Mondial" şi că pierderea acestei capacităţi în 1948 este „probabil cei mai semnificativă pierdere a serviciilor de informaţii din istoria Stateloi Unite". Pierderea a fost în cele din urmă atribuită spionului William Weisband, un lingvist rus de la Agenţia de Securitate a Forţelor Armate (predecesorul NSA). David A. Hatch şi Robert Louis Benson, 7/în *Korean War*: *The Sigint Background* (2000), www.nsa. gov/korea/ papers/sigint background korean war.htm. Dar fără accesul la arhivele secrete sovietice nu este

posibil să se determine precis răul făcut de spionul american John Walker, care a furnizat materiale criptografice maritime Uniunii Sovietice între 1968 şi 1985. În cel mai rău caz, se poate spune că materialele pe care Walker şi ceilalţi agenţi le-au furnizat KGB au oferit Uniunii Sovietice un „avantaj comparabil cu cel al Aliaţilor asupra naziştilor prin cunoaşterea Ultra. [Pe scurt, în cazul în care războiul ar fi izbucnit între cele două superputeri, Walker ar fi putut fi factorul decisiv pentru o victorie sovietică sau americană" Angelo Codevilla, *Informing Statecraft*: *Intelligence for a New Century* (Free Press, New York, 1992), pp. 176 – 178.

61. Pentru o discuţie exhaustivă despre comunicaţiile secrete ale marinei britanice în timpul Primului Război Mondial, vezi Patrick Beesley, *Boom 40*: *British Naval Intelligence 1914 – 18* (Harcourt Brace Jovanovich. New York, 1982).

62. Literatura referitoare la criptografia americană şi britanică în timpul celui de-al Doilea Război Mondial este enormă. Pentru o scurtă trecere în revistă, vezi G.J.A. OToole, *Honorable Treachery*: *A History of US Intelligence, Espionage, and Covert Action from the American Revol*ution *to the CIA* (Atlantic Monthly, New York, 1991), pp. 384 – 397.

M În mesajele lor, japonezii s-au referit la ţinta pe care o vizau ca *AF*. ofiţerii de informaţii din Hawaii au presupus că *AF* era codul pentru Midway, dar cei din Washington au crezut că poate fi vorba de altă locaţie, cum ar fi insula Johnston,

Oahu sau chiar coasta de Vest a Statelor Unite. Pentru a avea confirmarea că japonezii intenţionau să atace Midway, serviciile de comunicaţii ale marinei din Hawaii l-au pus pe comandantul american din Midway să trimită un mesaj către Hawaii conform căruia insula rămânea fără rezerve de apă. Aşa cum se anticipa, japonezii au interceptat mesajul şi două zile mai târziu o transmisiune radio japoneză (interceptată de Statele Unite) raporta către Tōkyō că rezervele de apă din *AF* erau scăzute, aceasta confirmând indirect că *AF* era într-adevăr Midway. Edwin T. Layton, Roger Pineau şi John Costello, „*And I Was There*”: *Pearl Harbor and Midway – Breaking the Secrets* (Morrow, New York, 1985), pp. 421 – 422.

m. Pentru o descriere a bătăliei şi a succesului serviciilor secrete din spatele acesteia, vezi Layton, „*And I Was There*”.

f»5. Vezi Comisia Specială pentru Activitatea Serviciilor de Informaţii a Senatului SUA, *Meeting the Espionage Challenge*: *A Review of United States Counterintelligence and Security Programs*, S. Rpt. 99 – 522 (Government Printing Office, Washington, DC, 1986), pp. 33 – 34, 80 – 81. În plus, Uniunea Sovietică a întreţinut mulţi ani (aşa cum Rusia a făcut-o până în 2002) un dispozitiv puternic de interceptare la Lourdes, Cuba. Având un personal de 1.500 de angajaţi ruşi, dispozitivul monitoriza traficul de voce şi date din SUA. O descriere a acestui dispozitiv se găseşte în secţiunea „Concluzii” a unui proiect de lege al Camerei Reprezentanţilor a Statelor Unite din 19 iulie 2000, „Russian-American Trust and

Cooperation Act of2.000", HR 4118, Congresul 106, sesiunea 2.

66. Peter Wright, fostul agent MI5, scrie în memoriile sale că „analiza traficului" era folosită de serviciile secrete sovietice pentru a reduce eficienţa eforturilor britanicilor de monitorizare a operaţiunilor secrete sovietice din Londra şi din împrejurimile acesteia. Aşa cum am menţionat anterior, sovieticii monitorizau comunicaţiile echipelor de supraveghere britanice din ambasada lor de la Londra. Faptul că aceste comunicaţii erau cifrate era nesemnificativ; dimpotrivă, le făcea „să iasă în evidenţă" în traficul radio necifrat din oraş. Prin analizarea acestor semnale radio, în special volumul activităţii radio, sovieticii puteau să deducă momentele în care operaţiunile de supraveghere ale contrainformaţiilor britanice (MI5) erau în derulare şi dacă una din operaţiunile lor era în pericol să fie compromisă din această cauză. După părerea lui Wright „ruşii culegeau majoritatea informaţiilor chiar din trafic, mai degrabă decât din conţinutul mesajelor". *Spycatcher*, pp. 52 – 53.

67. Vezi David Kahn, *Seizing the Enigma*: *The Race to Break the* (*Ithnm U-Boat Codes*, *1939 – 1943* (Houghton Mifflin, Boston, 1991), pp, 144.14* 215 – 216, 244 – 251 şi Patrick Beesly, *Very Special Intelligence*: *Thl of the Admiralty's Operational Intelligence Centre*, *1939 – 45* (DouMIÉB Garden City, NY, 1978), pp. 55 – 56, 97 – 98, 116, 195.

68. Pentru o descriere a acestei operaţiuni, vezi David E. Murphy, ftf Mgel A. Kondrashev şi

George Bailey, *Battleground Berlin*: *CIA vs. KÜ* & o *the Cold War* (Yale University Press, New Heaven, Conn., capitolul 11. Existenţa tunelului a fost trădată sovieticilor de către Oeoip» Blake, un spion sovietic în Serviciul Secret de Informaţii Britanic (*S\H*) \ cartea redă un raport al unei şedinţe de planificare SIS/CIA pe eeü Blake l-a furnizat sovieticilor (pp. 449 – 453) şi dezbate dacă sovieticii W folosit faptul că ştiau dinainte despre monitorizare pentru a induce I«eroare Statele Unite şi Marea Britanie (pp. 423 – 428).

69. Această operaţiune, cu numele de cod „Ivy Bells", este descrii! Im detaliu în cartea lui Sherry Sontag şi Cristopher Drew *Blând Mau Bluff*: *The Untold Story of American Submarine Espionage* (Public Affairs, New York, 1998), pp. 158 – 183, passim.

70. Wright, *Spycatcher*, pp. 81 – 86. Mai recent, serviciile secrete sovietU e au putut, din cauza practicilor deficiente în materie de securitate ale Statele Unite, să aibă acces la maşinile de scris electrice tri ml»* Ambasadei Americane din Moscova. (Departamentul de Stat al SUA în trimis maşini de scris în Uniunea Sovietică cu un transport comercial neînsoţit.) Prin înserarea unor dispozitive de interceptare sofisticate la maşinile de scris, sovieticii au putut să „citească" materialele (me crete sau nu) care erau scrise. Vezi US Senate, Select Committee ou Intelligence, *Meeting the Espionage Challenge*, pp. 34 – 35; pentru cu relatare neoficială a acestui episod vezi Kessler, *Moscow Station*, pp. 92 – 97.

71. Pentru o discuţie privind dificultăţile de

interceptare secretă a comunicaţiilor prin fibră optică, în special a celor ce trec prin ocean, ve/, 1 Neil King Jr., „As Technology Evolves, Spy Agency Struggles to Préserve Its Hearing”, *Wall Street Journal*, 23 mai 2001, p. Al.

72. De exemplu, în 2000 Select Committee on Intelligence a Senatului Statelor Unite a raportat: „Comitetul este din ce în ce mai îngrijorat de incapacitatea accentuată a National Security Agency (NSA) de a se ridica la nivelul provocărilor tehnologice şi de a le furniza liderilor americani informaţii SIGINT vitale”. *Report of the Senate Select Committee on Intelligence Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System and for Other Purposes*, S. Rep. 106 – 279, 4 mai 2000.

M Jeffrey Richelson, *Sword and Shield*: *The Soviet Intelllftent und Security Apparates* (Ballinger, Cambridge, Mass., 1986), pp 101.101 Vezi şi Curtis Peebles, *Guardians*: *Strategic Reconnatsanct* VmW/m * (Presidio, Novato, Calif., 1987), pp. 279 – 289. La (el ca natali”! da fotorecunoaştere, sateliţii *elint* au sarcini specifice de culegere a Informaţiilor care determină orbita şi numărul de sateliţi necesari, în generali localizarea *elint* şi urmărirea sistemelor militare ale altei ţări necesit! numeroşi sateliţi de altitudine joasă. Este probabil să se amplaseze pe o orbită elipsoidală un satelit pentru culegerea de informaţii *elint* în scopul de a determina caracteristicile electronice exacte ale unui sistem

militar. Pe o astfel de orbită satelitul, pe măsură ce se apropie de punctul cel mai îndepărtat de Pământ, pare să survoleze relativ încet zona-ţintă. Astfel, are mai mult timp să capteze şi să înregistreze semnalele dorite. Desigur, este posibil ca un satelit să se plaseze pe o orbită geosincronică. (Un satelit aflat pe o orbită geosincronică înconjoară Pământul pe deasupra Ecuatorului, realizând un cerc complet pe zi; astfel, de pe pământ pare să „atârne" inert deasupra unui anumit punct de pe Ecuator.) Aceasta permite receptorilor *elint* ai satelitului să stea „fixaţi" continuu deasupra unei ţări, dezavantajul fiind distanţa mare lată de transmiţnn cu i Aşadar, utilitatea unui sistem geosincronic depinde de intensitatea nom naiului receptat şi de sensibilitatea receptorilor de la bordul satelitului.

74. Calculul se face după cum urmează: unda radio emisă de un radar călătoreşte cu viteza luminii sau trei sute de mii de kilometri pe secundă. Aşadar, poate călători cu 300.000/500 = 600 km între impulsuri. Aşadar, dacă unda trebuie să atingă ţinta şi să se întoarcă la radar înainte ca următorul impuls să fie emis, ţinta nu poate fi la mai mult de trei sute de kilometri de radar. Jones, *The Wizard War*, p. 198.

75. Relatarea acestui episod este preluată din *The Electronic Spies* (Time-Life, Alexandria, Va., 1991), pp. 106 – 107.

76. Conform definiţiei oficiale dată de SUA, senzorii *masint* „includ, dar nu se limitează la sisteme radar, laser, infraroşu, acustice, nucleare,

de detectare a radiaţiilor, spectroradiometrice şi seismice, precum şi sisteme de recoltare a unor materiale lichide, solide şi gazoase" ale căror date, „când sunt colectate, procesate şi analizate, generează informaţii care detectează, recoltează, identifică sau descriu semnăturile (ea rac te risticile distincte) ale surselor-ţintă fixe şi dinamice". *Masint* a fost clasificat formal ca un domeniu al culegerii de informaţii în 1986, iar în 1993 DCI şi secretarul apărării au creat Central *Masint* Office (CMO) în cadrul Defence Intelligence Agency pentru a supraveghea şi a monitoriza activităţile de apărare *masint*. Vezi secţiunea 7, „MASINT: Measurement and Signals Intelligence", din US House of Representatives, Permanent Select Committee on Intelligence, 7C27: *Intelligence Community in the*

*21st Century* (US Government Printing Office, Washington, DC, 1«MHM www.fas.org/irp/congress/1996 rpt/ic21 /index.html.

77. Pentru o descriere generală a tehnologiei utilizate în monitori*»!** seismică în cazul testelor nucleare subterane, vezi US Congres». «Mi». of Technology Assessment, *Seismic Vérification of Nuclear* 7V4 fJtt *Treaties*, OTAISC-361 (Government Printing Office, Washington, IX\ mai 1988). Pentru detectarea de la distanţă a testelor nucleare la supr-uil", vezi Peebles, *Guardians*, pp. 331 – 342.

78. Pentru o descriere literară a culegerii de informaţii prin foloilr" sonarului, vezi Tom Clancy, *The Hunt for Red October* (Naval Institui»,

Annapolis, Md., 1984). Descrieri ştiinţifice sunt ceva mai greu de găitt în surse deschise. Totuşi, vezi Joël S. Witt, „Advances în Antisubmarin» Warfare”, *Scientific American*, februarie 1981. Pentru posibilitatea «l» detectare a submarinelor prin alte modalităţi, vezi Tom Stefanick, „The Nonacoustic Détection of Submarines”, *Scientific American*, martie 1988.

79. Practic, nu există niciun acord universal în virtutea căruia legislaţii! internaţională să permită recunoaşterea din satelit. Tratatul privi lui Spaţiul Cosmic din 1967, de exemplu, nu se referă direct la problema recunoaşterii din spaţiul cosmic. Tratatele privind controlul armamentului fac referire ia „mijloacele tehnice naţionale de verificare”, dar nu definesc aceşti termeni. De exemplu, articolul IX din Tratatul de neproliferare a armelor strategice din 1991 (între SUA şi fosta Uniune Sovietică) stipulează ca „mijloacele tehnice naţionale de verificare [mă fie folosite]... în conformitate cu principiile general recunoscute ale legislaţiei internaţionale”. Poziţia Statelor Unite a fost că suveranitatea unei naţiuni nu se extinde şi asupra spaţiului cosmic (adică dincolo de atmosfera terestră) şi, prin urmare, o naţiune este liberă să deruleze activităţi de recunoaştere din spaţiul cosmic, ca şi în largul mării. La începutul erei spaţiale opinia Uniunii Sovietice era că recunoaşterea din spaţiul cosmic era ilegală, la fel ca şi recunoaşterea aeriană, care implica survolarea neautorizată a teritoriului altei naţiuni. Totuşi, din motive obiective, folosirea efectivă a spaţiului de către un număr de state, inclusiv fosta

Uniune Sovietică, a făcut din problema ilegalităţii o temfl de dezbatere pentru dreptul internaţional.

80. Toate ţările ţin secrete costurile reale ale sistemelor implicate în recunoaşterea din spaţiul cosmic. Pentru o evaluare publică, vezi US Congress, Congressional Budget Office, *US Costs of Vérification and Compliance under Pending Arms Treaties* (Government Printing Office, Washington, DC 1990), pp. 43 – 47. Deoarece costurile de construire şi lansare a sateliţilor sunt mari, tendinţa a fost să se achiziţioneze câţiva sateliţi performanţi şi aceştia să fie configuraţi astfel încât să poată sta mult timp în spaţiu (poate şapte suu nun mulţi iuţii v HiittftH deşi economicoasă într-un fel, are dezavaiitaul (J) h»el* nu* în ut M Im „întuneric" în cazul în care se întâmplă ceva neaiumiai i «unul dlirtiv sateliţii ei sau dacă se întâmplă ceva într-o zonă din Imn» * $ HM p-nili acoperită uşor de orbitele sistemelor de recunoaşte i e cu hiente (I «Îi alegle mai flexibilă şi de perspectivă ar fi construirea mai multor «atei 1) 1 rM«l ieftini, cu durată de viaţă mai scurtă. În 1996, un studiu colectiv Permanent Committee on Intelligence a Camerei Reprezentanţilor tllit SUA menţiona că „transformările continue ale capacităţilor de procesare... permit amplasarea unor sateliţi care nu numai că suni mal uşori şi mai ieftini, ci şi mai inteligenţi... Pentru unele aplicaţii, la un moment dat «microsateliţii» amplasaţi în «nori»... ar putea implica culegerea distribuită şi divizarea sarcinilor, astfel permiţând reconstituirea sau înlocuirea anumitor părţi fără costuri prea mari. *IC21*: *Intelligence Community*

*in the 21st Century* (Government Printing Office, Washington, DC, 1996), p. 108, ww, fas.org/irp/congress/1996 rpt/ic21/index.html Totuşi, în general sateliţii mai ieftini sunt mai puţin eficienţi şi, oricum, lansarea presupune cele mai multe costuri. Alegerea strategici va fi determinată de priorităţile de culegere a datelor stabilite de guvern yl de rafinamentul tehnologiei deţinute de cei care construiesc sateliţii. Pentru o scurtă analiză a acestora şi a problemelor aferente, vezi Codevilla, *Informing Statecraft*, pp. 313 – 324.

81. Vezi Victor Suvorov, *Inside the Soviet Army* (Macmillan, New York, 1982), p. 106. Schimbări minore, dar imprevizibile ale traiectoriei pot fi realizate prin lovirea satelitului cu rachete de mici dimensiuni, numărul şi magnitudinea acestor manevre fiind limitate de capacitatea rezervorului de combustibil al satelitului.

X2. US Departament of Defense, *Conduct of the Persian Gulf War*, pp. 338, 710.

83. Citatele sunt dintr-o declaraţie comună a secretarului pe probleme de apărare al Statelor Unite, William Cohen, şi a generalului Henry II. Shelton, preşedintele Statului-Major Reunit, în faţa Comisiei pentru Serviciile Militare a Senatului Statelor Unite, 14 octombrie 1999, www.fas.org/man/dod-01/ops/docs99/blol41999 bt478 – 99.htm.

84. Pentru diferite variante de activităţi care se pot derula sub acoperirea unui camion obişnuit sau a unei dube, vezi Desmond Ball, „Soviet

Signals Intelligence: Vehicular Systems and Operations", *Intelligence and National Security*, 4, nr. 1 (ianuarie 1989), pp. 5 – 27. Pentru variante mai neconvenţionale, vezi Alfred Price, *The History of US Electronic Warfare*: *The Renaissance Years* (Association of Old Crows, Alexandria, Va., 1989), pp. 89, 160 – 161, pentru o descriere a proiectului US

Moonbounce, care intercepta semnalele radar sovietice reflectate de i Lună.

85. În plus, miniaturizarea permite Departamentului de Apărare al StatiltH Unite să dezvolte dispozitive de recunoaştere cât palma şi roboţi de cercetare miniaturali, pentru a fi folosiţi pe câmpul de luptă. Avioanele – spion de mici dimensiuni (numite „microaerovehicule" sau MAV) şi roboţii asigură unităţilor de luptă mici capacitatea de a cerceta iia»lua înconjurător. Michael A. Domhein, „Tiny Drones May Be Soldlei New Tool", *Aviation Week and Space Technology*, 8 iunie 1998, pp. 42.411, şi Kevin Kaley, „Robot Scouts May Gather Info for US Marine CorpiM, *Defense News*, 24 iulie 2000, p. 20.

86. Stansfield Turner, *Secrecy and Democracy*: *The CIA în Transi Ihm* (Houghton Mifflin, Boston, 1985; Harper and Row, New York, 198 n), p. 92. După Războiul Rece, Turner a susţinut că „Washingtonul poate construi cu uşurinţă un sistem care să detecteze orice activitate sem nificativă pe suprafaţa pământului, ziua sau noaptea, indiferent «i» condiţiile meteorologice sau topografice şi cu o asemenea frecventa, încât evitarea deliberată a acestuia ar fi

dificilă... Preţul de achiziţionate de cinci miliarde de dolari şi costurile de întreţinere de un miliard pe an... sunt un chilipir". În opinia fostului DCI, încă mai există loc pentru culegerea informaţiilor din surse umane în era de după Războiul Rece, dar, în general, „noua ordine mondială va genera sisteme tehnice care vor servi drept sabie, mijloace de ultimă oră în culegerea informaţiilor, iar operaţiunile de spionaj bazate pe surse umane vor fi floreta, fiecare fiind folosite judicios în funcţie de necesităţi". Turner, „Intelligence for a New World Order", *Foreign Affairs* 70, m. 4 (toamna 1991). pp. 151, 159.

87. În cei zece ani în care a lucrat pentru serviciile de informaţii americane, col. Ryszard J. Kuklinski, ofiţer în armata poloneză, a furnizat, printre altele, şi sute de pagini de documente secrete, inclusiv planurile de luptă sovietice pentru un război în Europa. Pentru relatări privind cariera de spion a colonelului Kuklinski, vezi Benjamin Weiser, „Polish Officer Was US s Window on Soviet War Plâns", *The Washington Post*, 27 septembrie 1992, p. Al, şi „A Question of Loyalty", *Washington Post Magazine*, 13 decembrie 1992, pp. 9 – 30.

88. Jozef Garlinski, *The Enigma War* (Scribner, New York, 1979), p. 16. Agentul german Hans-Thilo Schmidt a fost descris de istoricul David Kahn drept „spionul care a avut cea mai mare influenţă asupra sorţii celui de-al Doilea Război Mondial". *Kahn on Codes*: *Secrets of the New Cryptology* (Macmillan, New York, 1983), pp. 76 – 88.

89. *Humint* poate juca şi aici un rol. De exemplu, conform unor relatări, colonelul Kuklinski a furnizat informaţii despre care dintre „ţintele sovietice vizibile prin satelit erau false şi cuie erau «ulhviiomh Im piua, rapoartele lui Kuklinski au ajutat serviciile a n cu uium h an*! monitorizeze programul militar sovietic de consumi. a hhm ttllt fi huncăre de comandă şi control ascunse pe care aovlellell l alt apt Inf intenţionau să le folosească în cazul unui război tu Humpa tyzif, „Polish Officer Was US s Window on Soviet War Plâns”.

Jt). Vezi R. Jeffrey Smitli, „Iraq’s Secret A-Arms Effort: Lessoni for die World”, *The Washington Post*, 11 august 1991, p. Cl; R. Jeffrey Smith, „Iraq’s Nuclear Powers Underestimated by US”, *The Washington Post*, 13 noiembrie 1991, p. A45; R. Jeffrey Smith şi Glenn Frankel, „Saddam’s Nuclear Weapons Dream: A Lingering Nightmare”, *The Washington Post*, 13 noiembrie 1991, p. Al.

l. Smith, „Iraq’s Secret A-Arms”.

.». Pentru opinii privind roiul serviciilor secrete în „dezvoltarea sistemului militar”, vezi James R. Fitzăimonds, „Intelligence and the Revolution in Military Affairs”, în Roy Godson, Ernest R. May şi Gary Schmitt (eds.), *US Intelligence at the Crossroads*: *Agendas for Reform*, (Brassey’s [US], Washington, DC, 1995), pp. 265 – 287. Printre sarcinile care trebuie îndeplinite pentru a exploata la maximum *techint* în scopuri tactice, Fitzăimonds menţionează următoarele: „acoperire globală arie extinsă,

condiţii meteorologice diverse, identificare ziua/noaptea a ţintelor mobile şi fixe din zonele de coastă, în aer şi în spaţiu”; „monitorizarea continuă a ţintelor… în timp real (sau aproape în timp real)”, inclusiv „evaluarea consecinţelor războiului”; şi „transmiterea în timp real a informaţiilor privind localizarea ţintei către focosul rachetei, inclusiv către rachetele aflate în zbor” (p. 268).

93. Sherman Kent, *Strategic Intelligence for* American *World Policy* (Princeton University Press, Princeton NJ, 1949; reprint 1966), pp. 3 – 4. Kent, un veteran al Office of Strategic Services (OSS), serviciul secret american în timpul celui de-al Doilea Război Mondial, a oferit o teorie specific americană privind culegerea informaţiilor imediat după război.

94. V. Zaykin, „«Secret» Classification Removed”, *Izvestia*, 3 septembrie 1988, p. 2, retipărit şi tradus în Federal Broadcast Information Service (FBIS), *Soviet Report*, 8 septembrie 1988, (FBIS-SOV-88 – 174), pp. 53 – 54.

95. Campania strategică de bombardare a avut rezultate mixte. Spre meritul lor, economiştii OSS proiectaseră un sistem relativ sofisticat şi util de selectare a ţintelor. Dar au omis multe date de război privind economia germană care i-ar fi ajutat să-şi exploateze la maximum analiza straie Gică. Pentru aceste chestiuni, vezi Stephen Peter Rosen, *Wining the Next War*: *Inovation and the Modern Military* (Cornell University Press, Ithaca, NY, 1991), pp. 148 – 170.

96. Luându-se în considerare dependenţa totală a proiectului faţă de melenalele din surse deschise şi metodologiile ce, fiind elaborate în mediul academic, sunt cunoscute în ţara a cărei birocraţie a fost studiul A, ne putem întreba de ce această operaţiune trebuie efectuată de un serv le de la informaţii. Evident, nu este necesar, dar eventuala sa plasare iniţ în centru de cercetare public depinde de o serie de factori. Pe de o parte ar putea fi mai uşor să se recruteze personal pentru un astfel de ceitiftt deschis, iar activitatea sa ar fi mai uşor de împărtăşit comunllll academice. Pe de altă parte, procedurile speciale greoaie ar fi necomue pentru a integra acest material provenit din surse deschise în informell secrete sau pentru a le utiliza în activităţile derulate de serviciile secrete De exemplu, dacă informaţiile au fost necesare la recrutarea unul funcţionar pentru spionaj, solicitarea ar trebui camuflată, pentru a le ascunde motivul.

97. Donald E. Queller, *The Office of Ambassador* in the *Middle AgP** (Princeton University Press, Princeton, NJ, 1967), p. 90.

98. Lucrarea „Long Telegram”, scrisă de George Kennan în 1946, când em însărcinatul cu afaceri la Moscova, reprezintă un exemplu clasic de raport diplomatic de acest tip. Pe parcursul Războiului Rece, telegrama lui Kennan cu privire la Uniunea Sovietică a constituit temeiul intelecluat a ceea ce a devenit strategia americană de menţinere sub control a Uniunii Sovietice. Pentru textul telegramei lui Kennan, vezi Kenneth M Jensen (ed.), *Origins of the Cold*

*War*: *The Novikov, Kennan, atul Roberts»Long Telegrams" of 1946* (United States Institute of Peale, Washington, D.C, 1991).

99. În text este prezentată activitatea cotidiană a ataşatului militar, care la esenţă nu este secretă, deşi acesta ar putea încerca să călătorească în sau pe lângă zone restricţionate pentru a urmări obiective pe care ţara-gazdă ar prefera ca el să nu le urmărească. În plus, ca orice post diplomaţii, cel de ataşat militar poate fi folosit ca acoperire pentru un ofiţer de informaţii.

Capitolul 3: Ce înseamnă toate acestea? Analiza şi producerea informaţiilor

1. Acest aspect ridică întrebarea dacă se poate crea un cifru „imbatabil" Lăsând la o parte anumite consideraţii confuze privind natura caracterului aleatoriu, răspunsul este afirmativ: se poate crea un cifru imposibil de spart. Acest lucru implică utilizarea a ceea ce poartă denumirea „cod de unică folosinţă". De exemplu, să luăm în conn Itter ei» ui umtut ui «ititm care implică un cod supercifrat. Prima etapă conul A În it atttfiti umh în Mi cod a mesajului transmis. (Acest cod diferă de tel au, mai tiu lett ftfiinţ faptul că grupurile codului sunt numere formate din fu nu nit* l»tu din patru litere). De exemplu, cu ajutorul unul manual ttf mmlmM expresia „războiul începe mâine" ar putea fi codificaţi aut) fiu mă *4 ff f 1712.2844". În următoarea etapă, la aceste grupuri de iiuniet e li adaugi o serie de numere generate aleatoriu (cum ar fi „3041 S2$? am}i... îi luate în ordinea în care se regăsesc într-un tabel de numere, WR *Hm* după care au copii doar

expeditorul şi destinatarul, l’un adunate, obţinem:

4251.1112.284*4.3648.5217.815*0.7899.6329.0994

(Dacă suma depăşeşte 9999, se renunţă la primul „1”.) Apoi se trarutmite seria finală de grupuri de numere. La primire, procesul se în vei nea/a După ce-şi consultă copia codului care conţine grupele de numere aleatorii, destinatarul scade cifrele adăugate din cele pe care le primlie, obţinând primul set de numere, care apoi este decodat utilizând manualul de coduri. Sistemul se securizează în felul următor: după ce se utilizează o singură dată, hârtia cu o serie de numere aleatorii se distruge şi nu se mai utilizează niciodată. Dacă nu deţine „cheia” unui anumit mesaj, inamicul nu poate decripta mesajul, chiar dacă a obţinut manualul de coduri, întrucât cifrele adăugate nu au nicio legătură între ele. Prin urmare, numerele transmise nu vor prezenta un caracter sistematic pe baza căruia un criptanalist să poată sparge cifrul. Din păcate, „codul” (ale cărui copii trebuie furnizate în mod securizat atât expeditorului, cât şi destinatarului) trebuie să aibă cel puţin lungimea tuturor mesajelor care urmează să fie transmise. De aceea, sistemul nu este practic atunci când e dificil să se securizeze comunicaţiile dintre expeditor şi destinatar sau când este vorba despre un trafic mare de mesaje. Vezi John Karl Haynes şi Harvey Klehr, *Venona*: *Decoding Soviet espionage în AtMrilü* (Yale University Press, New Haven, Conn., 1999), capitolul 2, ce prezintă modul în care criptanaliştii americani au exploatat utilizarea defectuoasă de

către sovietici a sistemului codului de unică folosinţă pentru a citi mii de mesaje cu detalii referitoare la spionajul sovieticilor din Statele Unite.

Pentru cea mai amplă analiză publică a istoriei criptografiei, vezi David Kahn, *The Codebreakers*: *The* Story *of Secret Writing* (Macmillan, New York, 1967). Cu toate acestea, de la publicarea cărţii sale, dezvăluirea succeselor obţinute de britanici în spargerea cifrurilor germane în Hltithtl celui de-al Doilea Război Mondial au adăugat un capitol nou şi import«MJ la istoria criptografiei. Pentru aducerea la zi a lucrării lui Kahn...» *Kahn on Codes*: *Secrets of the New Criptology* (Macmillan, New 1983); vezi, printre alte eseuri, „The Spy Who Most Affected WirW War IF şi „Codebreaking în World War I and II The Major Sui iceftM, and Failures, Their Cauzes and Their Efects", pp. 76 – 88, 99 – 119, Vw» şi *Seizing the Enigma*: *The Race to Break the German U-Boat* (*ml* * 1939 – 1943*, de acelaşi autor (Houghton Mifflin, Boston, 1991).

3. Vezi Patrick Beesly, *Room 40*: *British Naval Intelligence 1914 IU* (Harcourt Brace Jovanovich, New York, 1982), pp. 3 – 7, 22 – 33.

4. Pentru o prezentare completă a acestui incident, vezi Barbara TVichitMM, *The Zimmermann Telegram* (Macmillan, New York, 1958, 1966).

5. Herbert O. Yardley, *The American Black Chamber* (Bobbs-Mcrrlll, Indianapolis, 1931; reeditare, Ballantine, New York, 1981), p. 4.

6. Kahn, *The Codebreakers*, p. 348.

7. O astfel de teorie matematică a fost elaborată la începutul anilor ’30 dl către criptografii matematicieni polonezi care au obţinut primele suceeie pentru Polonia şi apoi cele împotriva sistemului german Enigma. Ve/.l, de exemplu, Josef Garlinski, *The Enigma War* (Scribner, New York, 1979), pp. 25, 196 – 204.

8. Pe lângă cărţile citate deja, literatura include şi următoarele lucrări Peter Calvocoressi, *Top Secret Ultra* (Ballantine, New York, 1980); Josef Garlinkski, *The Enigma War*: *The Inside Story of the German Enigma Codes and How the Allies Brake Them* (Scribner, New York, 1979); Ronald Lewin, *Ultra Goes to War* (Hutchinson, Londra, 1978, McGraw-Hill, New York, 1978); F.W. Winterbotham, *The Ultra Secret* (Harper and Row, New York, 1974).

9. De exemplu, acum există o publicaţie cu circuit academic, intitulată *Cryptologia*, care abordează aceste subiecte.

10. Criptanalistul poate fi ajutat de numeroase posibile greşeli de utilizare a unui cifru. De exemplu, procedura germană de la începutul celui de-al doilea Război Mondial de repetare, la începutul fiecărui mesaj, a unei chei din trei litere a fost extrem de dăunătoare: pe criptanaliştii britanici i-a ajutat foarte mult faptul că ştiau că prima şi a patra literă ale unui text erau identice (la fel şi a doua şi a cincea, a treia şi a şasea). Pentru a vedea cum au exploatat britanicii această eroare a germanilor, vezi Gordon Welchman, *The Hut Six Story*: *Breaking the Enigma Codes* (McGraw-Hill, New York, 1982), pp.

59 – 73. La fel, formatele obişnuite ale mesajelor, saluturile standard sau alte expresii uzuale le pot furniza indicii importante criptanaliştilor. Welchman menţionează că el şi alţi criptanalişti britanici „l-au simpatizat pe un ofiţer german care a stat o perioadă mai lungă în Depresiunea Qattara din Noului Ah a ÎI l i apoMA zilnic că nu are nimic de raportat. În astfel de ca/ml, nu M viul îl ti solicităm comandanţilor britanici să-l lase în pace” (p, LU)

II De exemplu, s-a raportat că reţeaua de spionaj Walker a lui ni/u mm vi e iilor secrete sovietice o mare cantitate de material cifrat, ace Mea pui a ud astfel să decripteze un milion de mesaje secrete americane. Pentru o prezentare succintă a cazului Walker, vezi Christopher Andrew şi Oleg (îordievsky, *KGB*: *The Inside Story of its Foreign Operations from Lenin to Gorbachev* (HarperCollins, New York, 1990), pp. 524 – 531.

IKahn, *The Codebreakers*, p. 603; Ronald Lewin, *The American Magic*: *Codes*, *Ciphers and the Defeat of Japan* (Farrar Straus Giroux, New York, 1982), p. 113.

11, Kahn, *The Codebreakers*, p. 604.

14. Lewin, *The American Magic*, pp. 116 – 117. Pentru o discuţie despre acest incident, vezi şi Edwin T. Layton, „*And I Was There*”: *Pearl Harbor and Midway – Breaking the Secrets* (Morrow, New York, 1985), pp. 453 – 456.

15. Lewin, *The American Magic*, p. 117.

16. Dificultăţile de elaborare a unui nou sistem criptografic şi de distribuire a acestuia către cei implicaţi ar putea explica uşor de ce

japonezii n-au limitat să anunţe data unei schimbări de cod deja planificate. Mai mult, autorităţile japoneze au transmis ambasadei lor din Lisabona, Portugalia fiind neutră, că solicită „ziare, în special ziarul anti-guvernamentat *Chicago Tribune*, cu cât mai multe numere anterioare”. Deşi neconclu dent, acest lucru sugerează că autorităţile japoneze ştiau despre articolul din *Tribune* referitor la Midway şi că le preocupa îndeajuns de mult posibila sa semnificaţie pentru a dori să-l citească. Prezentarea succintă a informaţiilor secrete Magic (derivate din traficul telegramelor diplomatice japoneze interceptate), din 11 septembrie 1942, *apud* B. Nelson Macpherson, „The Compromise of US Navy Cryptanalysts alter the Battie of Midway”, *Intelligence and National Security*, 2, nr. 2, (aprilie 1987), p. 321. Prezentarea nu indică data mesajului transmis de la Tōkyō la Lisabona.

17. Christopher Andrew, *Her Majesty’s Secret Service*: *The Making of the British Intelligence Community* (Viking, New York, 1986), pp. 331 – 332.

18. Bob Woodward şi Patrick E. Tyler, „Libyan Cables Interceptând and Decoded”, *The Washington Post*, 15 aprilie 1986, p. Al.

19. Stephen Engleberg, „US Aides Worried over Libya Cables”, *The New York Times*, 17 aprilie 1986, p. A24.

20. Lewin, *Ultra Goes to War*, pp. 99 – 103. Vezi şi EH. Hinsley *et al*... *British Intelligence in the Second World War*: *Its Influence on Strategy and Operations* (Cambridge University Press, New

York, 1979), vol. 1, anexa 9 („Intelligence în advance of the GAF Raid on Cnvanut 14 November 1940"), pp. 528 – 548.

21. Pentru a face o analogie, vă puteţi imagina că vă confruntaţi cu UN de grafice care nu au nici inscripţii şi nici gradaţii pentru axele mi m» că vi s-a comunicat doar natura fenomenului ale cărui diferite ai petM sunt prezentate în grafice. Apoi, vi i se cere să explicaţi semnif Mfil fiecărui grafic şi să prezentaţi fenomenul în mod detaliat. Äfă * * menţionează Angelo Codevilla, „spre deosebire de inginerii care în proiectat-o, serviciul de informaţii ce interceptează telemetrie nu cunoaşte, aşa că trebuie să propună scala la care urmează să se cileattl fiecare canal" (Angelo Codevilla, *Informing Statecraft*: *Intelligent" fui a New Century* [Free Press, New York, 1992], p. 122.) Verificarea finală a propunerilor avansate şi a procesului ca un tot unitar connut i... producerea unui model de rachetă coerent ca structură care să curee pundă cu orice date obţinute din alte surse.

22. SALT II a interzis utilizarea criptării telemetrice dacă aceasta împiedU 11 verificarea modului în care se respectă prevederile tratatului. Unii nu argumentat că insistenţa Statelor Unite pe ideea includerii în tratat a acestei prevederi privind interzicerea criptării a avut efecte adverie întrucât Uniunea Sovietică a fost alertată cu privire la succesele obţinute de americani în interceptarea şi exploatarea telemetriei rachetelor sovietice Alţii au susţinut că succesele obţinute de spionajul sovietic împotriva sateliţilor americani

*sigint* „ar fi putut contribui la decizia sovietici lui de a cripta telemetria”. (Senatorul Gordon J. Humphrey, „Analysis and Compliance Enforcement” în William C. Potter [ed.], *Vérification aiul SALT*: *The Challenge of Strategic Deception* [Westriew, Bouldei, Colo., 1980], p. 112.) Pentru prezentări ale cazului de spionaj respectiv, vezi Robert Lindsey, *The Falcon and the Snowman* (Simon and Schusiei, New York, 1979), şi *Curtis Peebles*, *Guardians*: *Strategic Reconnaissante Satellites* (Presidio, Novato, Calif., 1987), pp. 200 – 201.

23. Dino Brugioni, el însuşi un fost PI, subliniază acest aspect în prezentarea pe care a făcut-o în cadrul unei informări extrem de importante din timpul crizei rachetelor din Cuba. El menţionează că persoana care a interpretat pentru prima dată fotografia şi care l-a informat pe Kennedy a înţeles că importanţa fotografiilor cu locaţiile rachetelor era mai mult decât evidentă şi s-a străduit să îl îndrume pe preşedinte pe parcursul analizei PI – iar în final, Kennedy a întrebat: „Sunteţi sigur?”. Brugioni, *Eyeball to Eyeball*: *The Inside Story of the Cuban Missile Crisix* (Random House, New York, 1991), p. 230.

24. „Rezoluţia la sol” se referă la capacitatea fotografiei de a reda un şablon standard abia distinct alcătuit din linii paralele în alb şi negru (adic;! linii şi spaţii) de aceeaşi lăţime. O distanţă a rezoluţiei la sol, de exemplu, de un picior (30, 48 cm) ar genera o fotografie în care şablonul având lăţimea liniilor şi spaţiilor de un picior este greu de distins. Un şablon de dimensiuni mai reduse, cu

o lăţime mai mică a liniilor şi spaţiilor, nu s-ar mai distinge deloc. (Această definiţie şi citatul din text sunt din Amrom Katz, „Observation Satellites: Problems and Prospects”, *Asâronautics* [aprilie 1960], pp. 5 – 6, o discuţie „în esenţă identică” cu cea din Amrom Katz, *Observation Satellites*: *Problems*, *Possibilities and Prospects*, RAND Paper P – 1707 [RAND, Santa Monica, Calif., 25 mai 1959].)

*IS*. Pentru o listă a rezoluţiilor la sol necesare pentru efectuarea analizei foto la diferite niveluri destinate mai multor tipuri de ţinte, vezi Amron Katz, „Tehnical Collection”, în Roy Godson (ed.), *Intelligence Requirements for the 1980’s*: *Clandestine Collection* (Naţional Strategy Information Center, Washington, DC, 1982), p. 109.

În Pentru o listă cu elementele de bază care se utilizează ia elaborarea unei semnături, vezi Brugioni, *Eyeball to Eyeball*, p. 196.

*11*. Pentru o discuţie legată de cratologie, vezi Robert S. Greenberger, „Can CIA Cratology Ultimately Outsmart Kremlin’s Shellology?”, *The Wall Street Journal*, 10 ianuarie 1985, p. Al.

.»X. Brugioni, *Eyeball to Eyeball*, pp. 104 – 105, 276 – 277.

29. Brugioni, *Eyeball to Eyeball*, pp. 538 – 548.

w). Robin Wright, „US Intelligence Failed to Warn of India’s Atom Tests”, *Los Angeles Times*, 13 mai 1998, p. Al, şi James Risen şi Tim Weiner, „US May Have Helped India Hide Its Nuclear Activity”, *The New York Times*, 25 mai 1998, p.

A3.

Îl sherman Kent, *Strategie Intelligence for* American *World Policy* (Princeton University Press, Princeton, NJ, 1949; reeditare, 1966), pp. 12 – 13, oferă cuprinsul unei cărţi referitoare la o ţară de interes, redactată în Germania pentru a fi utilizată în timpul celui de-al Doilea Război Mondial: „I. Condiţii generale. Locaţie. Frontiere. Zonă. Istorie. Structură guvernamentală şi administrativă; II. Caracteristicile ţării. Forme de relief. Soluri. Suprafaţa terenului. Climat. Aprovizionarea cu apă; III. Poporul. Naţionalităţi. Limbă. Atitudini. Distribuţia populaţiei. Aşezări. Sănătate. Structura societăţii; IV. Economia. Agricultură. Industrie. Afaceri şi Comer (Exploatări miniere. Pescuit; V. Transporturile. Căi ferate. Drumuri. Porturi. Aeroporturi. Căi navigabile fluviale; VI. Geografia militară [delimitare detaliată pe regiuni]; VII. Sistemul militar actual. Armata: ordinea de luptă; sisteme fixe de apărare, echipamente militare, aprovizionare. Flota militară: ordinea de luptă, flota, echipamente maritime de coastă, spaţiul aerian maritim, aviaţia militară: ordinea de luptă, flota aeriană militară, echipamente de zbor mai uşoare decât aerul, aprovizionare; VIII. Anexe speciale. Date biografice referitoare la membri importanţi ai guvernului. TerminiilH§fo’ geografică locală. Descrierea râurilor, lacurilor, canalelor. I. Um $ caracteristici ale centralelor electrice. Descrierea drumurilor, fum i aerodromurile şi principalele piste de aterizare. Listă cu principalele linii telefonice şi de telegraf. Bani,

unităţi de măsură. Plaje pl, mm operaţiuni militare derulate cu amfibii]".

32. House of Representatives, Committee on the Armed Services, *Ltwm Learned as a Result of the US Military Operations in Grenada*: *lieuiihi* Congresul al 98-lea, şedinţa a doua, 1984, H. Rept. 98 – 43, 24. Avênri în vedere faptul că administraţia Reagan şi-a exprimat în mod expie* îngrijorarea provocată de regimul marxist-leninist din Grenada, condu* de Maurice Bishop (ale cărui arestare şi executare de către colegii g au declanşat evenimentele şi apoi invazia), această lipsă a hărţilor şi a ni im date importante reprezintă un exemplu de eşec în anticiparea pollllell Statelor Unite.

33. Pentru o discuţie completă privind această sarcină, prezentată drept cu evitare a surprizelor rezervate de tehnologie, vezi Michael I. Handel, „Technological Surprinse în War", *Intelligence and National Security*, }, nr. 1 (ianuarie 1987), pp. l-53. Handel caracterizează în felul urmatul importanţa informaţiilor secrete ştiinţifice şi tehnice: „Mai mult dec Al oricare război anterior, războiul modern, ce are la bază dezvoltarea continuă a noilor sisteme de armament într-un ritm din ce în ce mai accelerat, depinde de informaţiile secrete... Chiar şi înainte de începerea luptei, deseori «bătălia serviciilor secrete» a decis cine a ieşit învingător şi cine a pierdut. Rolul pe care-l deţin informaţiile secrete ştiinţifice l tehnologice în război va creşte proporţional cu evoluţia tehnologica* a inamicilor şi cu modul cum utilizează aceştia armamentul de

ultimi oră" (p. 40).

34. R.V. Jones, *The Wizard War*: *British Scientific Intelligence, 1939 – 4*) (Coward, McCann and Geoghegan, New York, 1978), p. 104. Sistemul Knickebein presupunea două atene care transmiteau fascicule de unde radio unidirecţionale ce se intersectau deasupra ţintei bombardierelor, bombardierele germane zburau de-a lungul unui fascicul şi-şi lansau bombele când se intersectau cu celălalt. După ce au aflat de existenţa acestui sistem şi i-au stabilit caracteristicile, britanicii au iniţiat măsuri de contracarare – bruiaj şi lansarea unor fascicule false – care i-au diminuat eficienţa în mod semnificativ şi le-au zădărnicit trupelor germane eforturile de a efectua operaţiuni de bombardare a unor ţinte precise din Marea Britanie (pp. 127 – 128).

35. Eliot Cohen, „Analysis", în Roy Godson (ed.), *Intelligence Requirements for the 1990's*: *Collection, Analysis, Counterintelligence and Covert Action* (Heath, Lexington, Lexington, Mass., 1989), p. 82.

W» Jan Karl Tanenbaum, „French Estimâtes of (Set inimiv «i»utlittml Wm Plâns", în Ernest May (ed.), *Knowing One's* Mewiei *HUtHÊffÊÊ Assessment before the Two* World *Wars* (Princeton I uuve MME *fam*

Princeton, NJ, 1984), pp. 150 – 171.17. Lucrurile nu au stat neapărat aşa nici în cazul economiei hmv UMM»*, elfi permitea accesul analiştilor din serviciile secrete la dale n» pultl (cât, g le-ar fi putut oferi un avantaj faţă de alţi

experţi. Do oneuiplu, lu’ Ifrfri CIA a redactat o serie de studii privind industria petrolieri IMV letlel, anticipând că, până în 1985, producţia va scădea la opt fteee lullliMMte de barili pe zi, iar Uniunea Sovietică va importa între 3, 3 l 4, 1 tub/el Experţii din mediul academic şi de afaceri s-au arătat «copt lui fel de aceste rezultate, care într-adevăr s-au dovedit a fi departe de t eilllile în anii ’80, producţia de petrol sovietică a stagnat sau mi «proptit «I» 12 mb/zi. Pentru o analiză a acestei chestiuni care a stârnit ftimpill! generală faţă de CIA, vezi US Senate, Select Committee on Intellijienee, *The Soviet OU Situation*: *An Evaluation of CIA Analyses of Sovitt OII Production*: *Staff Report*, Congresul al 95-lea, şedinţa a doua, 1971, Committee Print. Pentru o analiză critică a activităţii derulate de aer vie îl le americane de informaţii pentru a evalua pe ansamblu economia fontei Uniuni Sovietice, vezi US Senate, Committee on Foreign Relation», *Estimating the Size and Growth of the Soviet Economy*: *Uninny*, Congresul al 101-lea, şedinţa a doua, 1990, S. Hrg. 101 – 1112.

38. Kent, *Strategic Intelligence*, pp. 7 – 8.

39. Uneori, serviciile de informaţii sunt considerate concurenţi ai presei, ceea ce este deseori în dezavantajul acestora. De exemplu, comunicatele de presă care anunţau că funcţionarii americani au urmărit lovitura de stat din Panamá din octombrie 1989 la CNN au insinuat că acest lucru era o dovadă a eşecului serviciilor de informaţii americane. Este o comparaţie incorectă, întrucât CIA nu are sarcina

de a furniza rapoarte de ultimă oră. Se pare că această critică a avut un oarecare impact. Vezi George Lardner Jr., „On This Network, All the News Is Top Secret: Defense Intelligence Agency Acts to Win Back Audience from CNN", *The Washington Post*, 3 martie 1992, p. Al, şi George Lardner Jr. l Walter Pincus, „Clearance Sought for New CIA Network: Agency Would Transmit Latest Intelligence Only to Select Top Officials", *Th* Washington Post*, *5* februarie 1992, p. Al.

40. Kent, *Strategic Intelligence*, p. 38.

41. Site-ul CIA Directorate of Intelligence (accesat pe 10 martie 2001): www.odei.gov/cia/di/work/daily.html.

42. Cord Meyer, *Pacing Reality*, *From World Federalism to the CIA* (Harpei and Row, New York, 1980), 352. Fostul DCI Robert Gates scria, în 1989: „De la un preşedinte la altul, PDB a cunoscut puţine modificări; câteva telegrame (între trei şi şase) ale DoS (Departament of Stato) l ale CIA de importanţă deosebită; ocazional, un raport cu informaţii necre Mp de la CIA, de la DIA sau de la NSA; anumite servicii prin cablu, rapoarte (rare) privind situaţia DoS ŞI CIA, în cazul crizelor din alte (III şi numeroase telegrame cuprinzând informări matinale aparţinând N M1 şi DoS". Din perspectiva lui Gates, adevărata schimbare radicali Im activitatea curentă a serviciilor de informaţii a constat în înfiinţarea de către administraţia Kennedy a White House Situation Room la începutul anilor '60. Anterior, „preşedintele se afla la mila aparatului birocraţi pe probleme de informaţii". Prin înfiinţarea White

House Situation Room, Departamentul de Stat, Departamentul pentru Apărare, CIA l NSA au început să le comunice preşedintelui şi echipei sale „informaţii secrete neevaluate sau brute, pe cale electronică”. Gates apreciază un această inovaţie a avut ca rezultat „diminuarea semnificativă a numărului de rapoarte informative înaintate Casei Albe de către CIA şi alte serviii de informaţii”. Robert Gates, „An Opportunity Unfulfilled: The llae and Perceptions of Intelligence at the White House”, *The Washington Quarterly* 12, nr. 1 (iarna 1989), p. 37.

43. Site-ul CIA Directorate of Intelligence. Pentru a ilustra atenţia acordat A de administraţia Clinton aspectelor economice ale problematicii internaţionale, începe să se publice *Economic Executives Intelligence Brief* (EEIB), cel de-al treilea cotidian care acoperă „aspecte problematice din acil vitatea directorilor economici, cum ar fi proceduri ale comerţului exterior, finanţări ilicite şi evoluţia unor companii energetice pe plan internaţional”.

44. US Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities [în continuare, Comisia Church], *Final Report*, vol. 1: *Foreign and Military Intelligence*, Congresul al 94-lea, şedinţa a doua, 1976, S. Rept. 94 – 755, 272 – 273.

45. Aveţi în vedere următoarea observaţie a unui înalt funcţionar al Departamentului de Stat american: „Ieri a venit la mine un prieten al meu din CIA să-mi dea o informare privind Germania de Est. Mi-a spus că şi-a citit materialul de trei ori

din cauza a ceea ce a auzit la radio, în timp ce se afla în maşină, pe drum, venind de la CIA către Departamentul de Stat". (Thomas L. Friedman, „In Quest for a Post Cold War Plan". *The New York Times*, 17 noiembrie 1989, p. A22). Această remarcă a demonstrat cât de rapide au fost transformările suferite de Europa de Est în noiembrie 1989, precum şi faptul că raportul analistului s-a axai în special pe cele mai recente evenimente şi mai puţin pe înţelegerea profundă a schimbărilor politice din Germania de Est.

46. Pentru o prezentare completă a analizei avertismentelor, vezi Timothy M. Laur, „Principles of Warning Intelligence", în Gerald W. Hopple şi Bruce W. Watson (ed.), *The Military Intelligence Community* (Westriew, Boulder, Colo., 1986), pp. 149 – 168.

47. Gordon Brook-Shepherd, *Storm Birds*: *Soviet Postwar Defectors* (Weidenfeld and Nicolson, New York, 1989), pp. 330 – 331, precum şi Christopher Andrew şi Oleg Gordievsky (eds.), *Instructions from the Centre*: *Top Secret Files on KGB Foreign Operations*, *1975 – 1985* (Hodder and Stoughton, Londra, 1991), pp. 67 – 90.

*H*. Conform ultimului decret privind activităţile serviciilor de informaţii din SUA (EO 12333, 4 decembrie 1981), „comunitatea serviciilor de informaţii" cuprinde CIA, NSA, DIA, „birouri din cadrul Departamentului Apărării care culeg informaţii secrete externe specializate prin intermediul programelor de recunoaştere", Biroul pentru Culegerea Informaţiilor şi Cercetare din cadrul Departamentului de Stat (IAR) şi

departamentele de culegere a informaţiilor din cadrul armatei, FBI şi Departamentele Trezorerie şi Energie (par. 3.4 [f]). Textul decretului este disponibil pe site-ul National Archives, www.nara. gov/fedreg/ codific/cos/e 12333.html.

19. Avi Shlaim, „Failures în National Intelligence Estimâtes: The Casc of the Yom Kippur War", *World Politics* 28, nr. 3 (aprilie 1976), pp. 368 – 369.

50. Alexander Orlov, *Handbook of Intelligence and Guerilla Warfant* (University of Michigan Press, Ann Arbor, 1965), p. 10. Cunoscând, *ne* pare, sistemul american, după cel de-al Doilea Război Mondial, Stalin a înfiinţat un birou unic de evaluare a informaţiilor secrete. Cu Unite acestea, având în vedere instrucţiile şi comportamentul anterior ale lui Stalin, era de aşteptat ca biroul respectiv să nu aibă acces la toate informaţiile, iar analizele sale să reflecte ceea ce dorea el tră aud A. (V.M. Zubok, „Soviet Intelligence and the Cold War: The «Smaln Committee of Information, 1952 – 1953", lucrarea a 4-a din cadrul Cold War History Project [Woodrow Wilson Center, Washington, DC, 19921). Comisia a fost desfiinţată în 1958. În ansamblu, există puţine materiale disponibile publicului cu privire la procesele de evaluare din alte (ftrl, cu excepţia Statelor Unite. Totuşi, pentru o prezentare ampli a titemulul britanic şi a istoriei sale organizatorice, vezi Reginald Hlbbert, „Intelligent i and Policy", *Intelligence and National Security*, 5, nr. I (Ianuarie 1990), pp. 110 – 127 şi Michael Herman, „Intelligence and Policy:

A Ctittinif lit". *Intelligence and National Security*, 6, nr. 1 (ianuarie 1991), Op, 229.2.19

51.Barton Whaley, *Codeword Barbarossa* (MIT, Cambridge, 197.1). Shlaim, „Failures în National Intelligence Estimatoa", pp, 3411 i Ht), Michael I. Handel, *Perception, Deception and şut pu s-int* Gif* *of the Yom Kippur War* (Leonard Davis Institute for Internatum Al Wallon*, Jerusalem Paper 19, Ierusalim, 1976); Eliot Cohen l Jttitn Ctooch.

*Military Misfortunes*: *The Anatomy of Failure în War* (Free Prem, Ne* York, 1990), capitolul 5 („Failure to Anticipate: Israeli Defence Hutn* on the Suez Front and the Golan Heights, 1973"), pp. 95 – 131; Roheite Wohistetter, *Pearl Harbor*: *Warning and Décision* (Stanford Univeiilt* Press, Stanford, Calif., 1962); Edwin T. Layton, *„And I ms Thmm Pearl Harbor and Midway – Breaking the Secrets* (Morrow, New Yoili, 1985); Gordon W. Prange *et al*, *At Dawn We Slept*: *The Untold Stm of Pearl Harbor* (McGraw-Hill, New York, 1981); şi, în general, Klaut Knorr şi Patrick Morgan (eds.), *Strategie Military Surprinse*: *Incenttvpi and Opportunities* (Transaction, New Brunswick, NJ, 1983).

52. Vezi Harvey de Weerd, „Strategie Surprinse in the Korean War", *Orht*-l 6, nr. 3 (toamna 1962), pp. 435 – 452 şi Eliot Cohen, „«Only Half nu-Battle»: American Intelligence and the Chinese Intervention in Korea, 1950", *Intelligence and National Security*, 5, nr. 1 (ianuarie 1990), pp. 129 – 149. Pentru ofensiva din Ardeni, vezi Charles B. MacDonalil, *A Time for*

*Trumpets*: *The Untold Story of the Battle of the Bult* (Morrow, New York, 1985), pp. 17 – 92, şi Hinsley *et* al, *British Intelligence in the Second World War*, vol. 3, pentru 2, pp. 402 – 438. Pentru ofensiva Tet, vezi James J. Wirtz, *The Tet Offensive*: *Intelligence Failun» în War* (Cornell University Press, Ithaca, NY, 1991).

53. Lewin, *Ultra Goes to War*, pp. 317 – 318.

54. La momentul respectiv, acest eşec a fost considerat suficient de distructiv pentru ca preşedintele Carter să le trimită o notă scrisă de mână lui Cyrus Vance, Zbigniew Brzeziński şi Stansfield Turner (secretar de stat, consilier prezidenţial pe probleme de securitate naţională şi, respectiv, director ai serviciului central de informaţii), în care a specificat, cu o francheţe necaracteristică birocraţiei guvernamentale: „Nu sunt mulţumit de calitatea rapoartelor noastre politice". Stansfield Turner, *Secrecy and Democracy*: *The CIA în Transition* (Houghton Mifflin, Boston, 1985, Harper and Row, New York, 1986), p. 113. Vezi şi House of Representatives, Permanent Select Committee on Intelligence, Surjcommittee on Evaluation, *Iran*: *Evaluation of US Intelligence Performance prior to November 1978*: *Staff Report*, Congresul al 96-lea, şedinţa 1, 1979.

55. Un raport al Comisiei Senatului Statelor Unite privind serviciile de informaţii susţine că „problema nivelurilor preţului petrolului a fost analizată în cadrul restrâns cerere-ofertă, care tindea să amplifice atât influenţele politice, cât şi anumiţi factori economici, cum ar fi flexibilitatea

cererii şi a ofertei”. Raportul pretinde şi că „aspectele politice ale relaţiilor dintre statele membre ale OPEC şi dinamica internă a guvernului saudit... nu au fost integrate în mod consecvent în evaluarea economică a comunităţii” (Select Committee on Intelligence, Surxommittec on Collection, Production and Quality, *US Intelligence Analysis and the*

*OU Issue, 1973 – 1974*: *Staff Report*, Congresul «I 91 Im Mut*«Muei 1977, Committee Print, 4, 5). Aceasta sugercază i A mm îl şi îl pe păinteft» de securitate implicaţi au elaborat o analiză economii A prea inuat M l în consecinţă, apolitică.

56. Campania peninsulară din timpul Războiului Civil, conduri 4» gfWHtul George McClellan în primăvara şi vara anului 1N62, rptelhti HM

exemplu clasic de eşec al serviciilor de informaţii M» Hellen fu deplasat armata unională alcătuită din 85.000 de combatanţi pe mate ftf la Washington în peninsula formată de râurile James şi Ybrk «Un Virginia El intenţiona să avanseze în interiorul peninsulei şi HA ocupe M h Iun» mii (capitala Confederaţiei), punând astfel capăt războiului Cu Uliii acestea, la Yorktown, McClellan s-a lovit de rezistenta Confederaţiei Pe baza informaţiilor secrete furnizate în mare parte de celebru) detfetiv particular Allan Pinkerton, McClellan a crezut că va înfrunta UM imuni» redutabil; de fapt, era vorba despre 17.000 de soldaţi ai Confederaţiei, dispuşi pe un front de opt mile. În loc să atace şi să spargi frontul

Confederaţiei, McClellan a preferat asediul de lungă duraţi, Cin i oferit Sudului timp suficient pentru a se regrupa. În primfivari l în vară, atât armata unională, cât şi cea a Confederaţiei yl au aporii efectivele. Dar încă o dată, bazându-se pe informaţii secrete incorecte, McClellan a fost sigur că se confruntă cu o armată a sudiştilor format A din 200.000 de combatanţi; de fapt, era vorba de numai uei sferturi din propria armată de 112.000 de soldaţi. În august, crezând că este cu mult depăşit din punct de vedere numeric, generalul McClellan a abandonat campania şi, prin aceasta, şansa optimă de a obţine o posibilă victorie rapidă asupra Sudului. Vezi CT. Schmidt, „G-2, Army of the Potomac", *Military Review*, 28 (iulie 1948), pp. 45 – 56 şi Edwin C. Fishel, „Pinkerton and McClellan: Who Deceived Whom? *Civil War Îiis tory*, 34, nr. 2 (iunie 1988), pp. 115 – 142.

Un alt exemplu mai concludent este al lui Williamson Murray, care a argumentat că evaluările defectuoase realizate de Franţa şi Marca I ti în nain ceea ce priveşte echilibrul de forţe din Europa în perioada 1938 – 1939 au făcut ca aceste două ţări să nu fructifice momentele avantajoase de atunci, pentru a obţine o victorie mai puţin costisitoare (comparativ cu ceea ce a urmat) împotriva Germaniei naziste. Williamson Murray, *The Change* in the *European Balance of Power*, *1938 – 1939*: *The Puth to Ruin* (Princeton University Press, Princeton, NJ, 1984).

57. Au existat elemente de surpriză tactică, de exemplu, în dispunerea de către Aliaţi a

porturilor artificiale, care să fie utilizate până la capturarea unor porturi importante, cum ar fi Cherbourg. Pentru o dezbatere pe marginea problemei pe care o reprezentau aceste porturi artificiale pentru serviciile de informaţii germane, vezi Handel, „Technologa al Surprinse în War”, pp. 14 – 15.

58. Vezi Cohen, „Only Half the Battle”. Cohen susţine că, deşi este pimilill ca atacul chinezilor să fi luat prin surprindere conducerea poliţiefl»I«I«Washington, generalul MacArthur, comandantul armatei americane l al trupelor ONU, ştia despre infiltrarea masivă a trupelor chinouo în Coreea; dezastrul nu a fost provocat atât de surpriză, cât de aplicai ea tacticilor necorespunzătoare împotriva armatei chineze. Generalul MacArthur a crezut că SUA puteau să profite de supremaţia deţinuia la atacurile aeriene şi în lupta sa împotriva Armatei de Eliberai o a Poporului Chinez, cât şi împotriva Armatei Poporului Nord-Corcoan în cele din urmă, această opinie eronată a reflectat o greşeală de evaluat» a diferenţelor dintre armata coreeană, bine dotată din punct de vedere tehnic şi deci limitată la deplasarea rutieră (după modelul sovietic), şi cea chineză, fără echipamente mecanizate, ale cărui trupe dispersate de infanterie nu au constituit ţinte eficiente pentru atacurile aeriene.

59. Lewin, *Ultra Goes to War*, pp. 347 – 351.

60. John Prados, *The Soviet Estimate*: *US Intelligence Analysis and Russian Military Strength* (Dial, New York, 1982), pp. 41 – 50, 76 – 95, 111 – 126.

61. Albert Wohistetter, „Is There A Strategie Arms Race? „Foreign Policy, nr. 15 (vara anului 1974): 3 – 20 şi „Rivals, but not Race", Foreign Pölicy, nr. 16 (toamna anului 1974); 48 – 81.

62. De exemplu, Donald Rumsfeld, care în 1998 a devenit preşedintele Comisiei de Evaluare a Ameninţărilor cu Rachete Balistice asupra Statelor Unite, a susţinut că un NIE anterior a subestimat ameninţarea respectivă pentru că, printre altele, analiştii care s-au ocupat de acest subiect nu au avut acces la informaţiile privind transferul de tehnologic între diferite state. În consecinţă, evaluarea lor privind perioada în care anumite ţări vor construi rachete balistice capabile să atace Statele Unite a avut la bază perioada în care ele vor putea construi tehnologie cu resurse interne. Întrucât a avut acces la informaţii privind transferul de tehnologie, Comisia a ajuns la concluzia că unele dintre aceste ţări ar putea reprezenta în scurt timp o ameninţare împotriva Statelor Unite din cauza deţinerii unor rachete balistice. Eric Schmitt, „Panel Says US Forces Risk a Surprinse Missile Attack", *New York Times*, 16 iulie 1998, p. A24, şi *The News Hour with Jim Lehrer*, 15 iulie 1998, interviu cu Donald Rumsfeld.

63. Norman Schwarzkopf, *It Doesn't Take a Hero*: *The Autobiography* (Bantam, New York, 1992), p. 293; Bob Woodward, *The Commanders* (Simon and Schuster, New York, 1991), pp. 205 – 208, 215; Bruce W. Jensen, *With Friends Like These*: *Reagan, Bush and Saddam, 1982—1990* (Norton, New York, 1994), pp. 173 – 174.

m Wesley K. Wark, *The Ultimate Enemy*: *British Intelligence and Nat.v Germany*, *1933 – 1939* (Cornell University Press, Ithaca. NY, IMÂS), pp. 228 – 229.

(*6*. Acest aspect este similar problemei legate de „modificarea paradigmei” abordată în filosofia ştiinţei – adică felul în care un cadru de organizare, precum fizica newtoniană, dă naştere altui cadru de organizare (de exemplu, relativitatea). Cu toate acestea, trebuie evidenţiate două diferenţe importante, care sugerează că modificarea paradigmei poate avea loc mai uşor atunci când este vorba despre o teorie ştiinţifică decât în cazul analizei informaţiilor secrete: 1) pionierii noilor idei nu au nevoie nici măcar de îngăduinţa, cu atât mai puţin de acordul adepţilor vechilor concepţii pentru a-şi publica opiniile, 2) pot fi elaborate şi efectuate experimente special concepute pentru a se adopta una dintre cele două variante de concepţii. Chiar şi aşa, unii au pretins că modificările nu sunt atât rezultatul adoptării noilor idei de către oamenii de ştiinţă din domeniu, cât al adoptării acestora de către nou-veniţii în disciplina respectivă.

66. Uneori, acest mecanism este desemnat de termenul *proiecţie*, specific domeniului psihologiei, care, în sens mai tehnic, înseamnă mecanismul psihologic prin care un subiect îi atribuie altui subiect sentimente sau caracteristici (precum ostilitatea şi reaua-credinţă) pe care nu le agreează la propria persoană şi pe care vrea să le renege. Întrucât, în anumite cazuri, acest mecanism poate reprezenta baza psihologică a

imaginii în oglindă, cele două concepte, care acţionează la niveluri diferite, nu sunt identice; de exemplu, proiecţia nu poate fi cauza faptului de a-i atribui în mod eronat unui inamic o caracteristică (de exemplu, împăcarea şi mulţumirea faţă de *status quo*) pe care o are şi de care este mulţumit.

67. Eşecul serviciilor de informaţii israeliene în acest caz este abordat în Shlaim, „Failures în National Intelligence Estimâtes". Shlaim opinează că, în faţa probelor privind un potenţial atac, serviciile de informaţii israeliene şi-au menţinut „concepţia" sau ideea că Egiptul nu va ataca până când nu va fi capabil să organizeze atacuri aeriene ample pentru a distruge forţele aeriene israeliene, iar Siria nu va ataca fără Fajipt. Prima şi cea mai importantă parte a acestei concepţii reflectă, la nivel militar, aceeaşi imagine în oglindă existentă la nivel politic – convingerea că Egiptul nu va declanşa un război pe care nu are şanse reale să i câştige. Totuşi, în analiza lor referitoare la războiul din 1973(*Military Misfortunes*, capitolul 5), Cohen şi Gooch susţinea această „concepţie" nu s-a bazat doar pe perspectiva imaginii în oglindă. Israelul a avut probe relativ recente referitoare la evaluarea făcută de Egipt cu privire la resursele necesare pentru a câştiga războiul (p. 116). Prin urmare, în acest caz, eşecul analitic nu a pornit de la perspectiva imaginii în oglindă la nivel militar, ci de la imposibilitatea de a se preconlaa i Egiptul şi-ar putea modifica noţiunea de *succes strategic* (sucée* tu privire la obiectivele politice generale ale unui război, pp. 123 ÎJM) Acest eşec pare să indice o imagine în

oglindă la nivel politic.

68. *Al-Hamishmar*, 14 septembrie 1975, *apud* Shlaim, „Failures în National Intelligence Estimâtes”, p. 362.

69. Acest pasaj a fost şters din versiunea finală a NIE, dar a continuat «I existe sub forma unei note de subsol care exprima opiniile diferite ăla directorului IAR din cadrul Departamentului de Stat. Church Commitee, *Final Report*, vol. 1, p. 78. Textul complet al NIE este disponibil ttt Donald Steury (ed.), *Intentions and Capabilities*: *Estimâtes on Soviet Strategic Forces*, *1950 – 1983* (Center for Study of Intelligence, CIA, Washington, DC, 1996), pp. 253 – 261. Nota de subsol apare la pagina 261.

70. Jones, *The Wizard War*, p. 457.

71. Jones, *The Wizard War*, p. 458. Evoluţiile înregistrate de tehnologia radar înaintea celui de-al Doilea Război Mondial oferă două exemple interesante de eşec al evaluării diferenţelor dintre abordarea inamicului privind o anumită problemă tehnică şi abordarea proprie. La mijlocul anilor ’30, atât Marea Britanie, cât şi Germania demonstraseră est detectarea la distanţă a avioanelor s-a putut realiza prin utilizarea transmisiilor radio (radar). Cu toate acestea, niciuna dintre aceste ţări nu a ştiut că şi cealaltă a aflat „secretul” radarului, deşi amândouă realizaseră şi puseseră în practică sistemele până în 1939. În absenta detectării unei transmisii radar germane, comunitatea tehnică şi de informaţii britanică a respins toate dovezile (fotografice sau umane) est Germania ar fi deţinut

radare. Nu s-a detectat niciun semnal întrucât Germania inventase radare cu mult diferite de cele britanice. În multe privinţe, radarele germane erau mai bune, dar aveau un defect: rază de acţiune limitată. Ca urmare, semnalele radar nu au fost detectate în Marea Britanie doar pentru că erau prea slabe pentru a fi detectate de la mare distanţă. Comunitatea specialiştilor germani în domeniul tehnicii era mai puţin convinsă decât cea britanică de faptul că doar radarul în sine constituia „o minune a tehnicii". În consecinţă, germanii s-au străduit să capteze semnale ale britanicilor. Întrucât căutau un semnal similar cu al lor, au stabilit în mod eronat că semnalele radar captate de ei proveneau de la reţeaua britanică de curent electric; de fapt, britanicii nu fuseseră capabili să producă un semnal atât de performant şi concepuseră unde radar diferite, dar tot eficiente. Din cauza acestei erori de analiză, Luftwaffe nu a produs echipamentul necesar pentru a contracara la timp radarele britanice în Bătălia Angliei, oferind astfel Forţelor Aeriene Regale un avantaj semnificativ în spaţiul aerian al

Marii Britanii. Jack Nissen şi A.W. Cockeilll, *WIHH lty lh*ş *Ibéit* ttttf (Robert Hale, Londra, 1989), pp. 17 – 39, *! Jone*, *IH0* H9 hM MNR pp. 189 – 202.

*12*. În principiu, putem vorbi despre eşecuri tu 1 un, a în m ihfn „ntiţillin secrete; cu toate acestea, rareori auzim de ele, mal «le» Inutil îM 1 t»l* mai interesante cazuri sunt cele în care informaţiile de Interni «mm *é*ş fapt disponibile.

73. În măsura în care serviciile de informaţii

se preocupă mai puţin de aspectele politice şi militare şi mai mult de cele economice ţfl nodale (cum a sugerat, de exemplu, William Colby, fostul director al CIA, 9I după cum s-a discutat în capitolul 7), această afirmaţie este mai puţin convingătoare. Un serviciu de informaţii care se ocupă în special de elaborarea prognozelor socioeconomice poate descoperi că adversarii săi nu sunt interesaţi de progresele înregistrate de serviciu şi nu doresc să-l obstrucţioneze în vreun fel. (Dar nu neapărat: în anii ’20, sovieticii s-au străduit să convingă serviciile de informaţii occidentale că în URSS comunismul dispare, iar liderii acestuia adoptă un naţionalism Inofoilllv. John J. Dziak, *Chekistry*: *A History of the KGB* [Heath, Lexlngton, Lexington, Mass., 1988], p. 48.) în mod similar, uneori se vrea ca inamicul să înţeleagă situaţia în mod corect. De exemplu, strategia de construire a unui scut de arme nucleare (presupunând că un stat dispune de forţele necesare pentru a o pune în practică şi că nu este vorba despre un bluf) depinde de evaluarea corectă făcută de către alt guvern, care stabileşte că, după primul atac, armata respectivă va mai putea provoca pagube imense ţării sale. Aşa s-a întâmplat în toamna şi iarna anului 1961, când, printr-o serie de discursuri şi articole de ziare, înalţi funcţionari din administraţia Kennedy le-au comunicat în mod intenţionat sovieticilor că SUA nu mai au nicio îndoială cu privire la superioritatea lor în domeniul armamentului nuclear. Bazându-se pe capacitatea sa de a „descifra” secretele armatei sovietice, guvernul

american ştia că nu mai exista nicio „diferenţă în ceea ce priveşte rachetele” şi că deţine arme mai mult decât suficiente pentru a declanşa a doua ofoniivi devastatoare împotriva Uniunii Sovietice, în eventualitatea izbucnirii războiului. Vezi Prados, *The Soviet Estimate*, p. 172.

74. US Senate, Select Committee on Intelligence, Subcommittee on Collection. Production and Quality, *The National Intelligence Estimâtes A-B Te-am Episode Concerning Soviet Strategic Capability and Obiectives*, Con greşul al 95-lea, şedinţa a doua, 1978, Committee Print. (Partea din raportul echipei A-B privind intenţiile strategice ale sovieticilor a fost publicată în 1992 într-o formă revizuită de CIA.)

75. Mandatul Congresului de înfiinţare a comisiei bipartite a survenit după două evaluări prealabile ale NIE, ambele considerând că analiza cuprinsă în NIE este defectuoasă. US Senate, Select Committee on Intelligent* *Hearing on Intelligence Analysis on the Long-Range Missile Thmil* H» *the United States*, 4 decembrie 1996, www.fas, org, irp/congress/1996 lu’/ index.html; „Foreign Missile Threats: Analytic Soundness of CertalH National Intelligence Estimâtes”, GAO Letter Report (GAO/NSAJD-96 – 211), 30 august 1996, www.fas.org/irp/gao/nsi96225.htm; *Report of tht Commission to Assess the Ballistic Missile Threat of the United Staţie* 15 iulie 1998, www.fas.org/irp/threat/bm-tlireat.htm. 76. Potrivit lui Shlomo Gazit, serviciile militare secrete israeliene se fblottetK în mod curent de un „avocat al diavolului” în eforturile de încurajate a

unei atitudini mai deschise în procesul analitic. Shlomo Ga/.lt, „Estimâtes and Fortune-Telling în Intelligence Work”, *International Security*, 4, nr. 4 (primăvara 1980), p. 40, n. 3. În anul 1985, Statele Unite au folosit o abordare de tip „avocatul diavolului” pentru a reanali/a problema complicităţii sovietice la încercarea de asasinare a Papei Inan Paul al II-lea din 1981. În perioada imediat următoare atacului, CIA era de părere că tentativa de asasinat trebuia pusă pe seama unui singur individ. În 1985, conform unor noi informaţii, ţinute secrete până în acel moment, era posibil ca Bulgaria şi Uniunea Sovietică să fi fost implicate în atacul împotriva Papei; astfel, Robert Gates, adjunctul DCI, a ordonat elaborarea unei evaluări în stilul tipic „avocatului diavolului” pentru a aduce argumente în favoarea implicării Uniunii Sovietice. Această evaluare a fost folosită în timpul audierilor de cătrr cei care se opuneau nominalizării lui Gates, ca exemplu al presupusei lui disponibilităţi de a modifica o analiză astfel încât aceasta să corespundă opiniilor generale ale membrilor administraţiei. După cum sugerează această controversă (precum şi exerciţiul Echipei A-B, care s-a desfăşurat înaintea acesteia), încercarea de a folosi o abordare de tip „avocatul diavolului” pentru analiza unui singur aspect poate fi foarte uşor criticată ca fiind un efort de a politiza analizele realizate de serviciile secrete. US Senate, Select Committee on Intelligence, *Nomination of Robert Gates to be Director of Central Intelligence*: *Hearings*, 102 d Cong., prima şedinţă, 1991, S. Hrg. 102 – 799: vol. 1, p, 637;

vol. 2, pp. 347 fi., 619; vol. 3, pp. 62 – 118. Benjamin Weiser, „Papal-Shooting Analysis: Case Study în Sianting?”, *The Washington Post*, 1 octombrie 1991, p. A8. Comisia Rumsfeld s-a format în urma unei controverse referitoare la utilizarea de către Statele Unite a unui sistem de apărare împotriva rachetelor balistice. Totuşi, Comisia a scăpat de acuzaţia de politizare, deoarece membrii acesteia (printre care se numărau experţi din ambele tabere) au căzut de acord, în mod unanim, asupra raportului final. Comisia a fost ajutată şi de faptul că, la scurt timp după emiterea raportului din iulie 1998, Coreea de Nord a lansat o rachetă considerată a fi capabilă să lovească Alaska sau Hawaii.

77. Richard K. Betts, „Analysis, War, and Décision: Why Intelligent e Failures Are Inévitable”, *World Politics*, 31, nr. 1 (octombrie 1V7M), pp. 61 – 89.

Capitolul 4. În culise: operaţiunile secrete

1. Legea privind autorizarea activităţii serviciilor de informaţii, anul fiscal 1991, L. 102 – 88, 14 august 1991 [50 USC 413 b].

2. Activităţile secrete au fost „definite” pentru prima dată în 1974 prin Amendamentul Hughes-Ryan (Secţiunea 662 din Legea privind asistenţa externă din 1961 [22 USC 2242]). Acest act normativ nu oferea o definiţie în sensul strict al cuvântului; dar le cerea preşedinţilor să autorizeze în mod explicit şi apoi să raporteze Congresului, toate „operaţiunile [inclusiv cheltuielile realizate de către sau în numele CIA) efectuate în state străine, altele decât cele care au

ca scop obţinerea unor informaţii secrete”. Până în 1991, definirea activităţilor secrete (sau a „acţiunilor speciale”, după cum mai sunt numite) a fost in-am spre a fi interpretată ulterior în decretele şi directivele prezidenţia Io emise de comisiile de supraveghere ale Congresului. Pentru o sinteză a evoluţiei definiţiei acţiunilor sub acoperire anterioare anului 1991, vezi Americo R. Cinquegrana, „Dancing in the Dark: Accepting the Invitation to Struggle in the Context of «Covert Action», the Iran-Contra Affair and the Intelligence Oversight Process”, *Houston Journal of International Law*, 11, nr. 1 (toamna 1988), pp. 177 – 209.

3. John Bruce Lockhart, fost reprezentant al Ministerului de Externe britanic cu o vastă experienţă în domeniul serviciilor secrete, foloseşte sintagma *acţiune politică specială* ca sinonim pentru acţiunile secrete; această expresie este folosită, probabil, în engleza britanică. John Bruce Lockhart, „Intelligence: A British View”, în K.G. Robertson (ed.), *Approaches to Intelligence* (Macmillan, Londra, 1978), pp. 37, 46.

4. Această definiţie a măsurilor active este preluată din Richard II. ShultX Şi Roy Godson, *Dezinformatsia*: *Active Measures în Soviet Strategy* (Pergamon-Brassey’s, McLean, Va., 1984), p. 193.

5. În Statele Unite a apărut sintagma *diplomaţie publica*, acoperind unele dintre tehnicile măsurilor active. Statele Unite nu au creat însă structurile organizatorice care să permită aplicarea acestui concept. Directiva 77 a

Deciziei de Securitate Naţională (NSDD-77), din 14 ianuarie 1983, defineşte, în linii mari, diplomaţia publică, referindu-se la aceasta drept „acţiuni ale guvernului american menite să sprijine obiectivele noastre de securitate naţională”.

@6. În lucrarea lor privind CIA, Victor Marchetti şi John D. Marks s-au referit într-un mod critic la un program de antrenament pentru poliţie, care se desfăşura în Sudul Vietnamului; oricum, cea mai mare nemulţumire a lor este legată de implicarea unei instituţii academice, şi anume Michigan State University, într-un program secret. Victor Marchetti şi John D. Marks, *The CIA and the Cult of Intelligence* (Knopf, New York, 1974), p. 234.

7. Secţiunea 660 a Legii privind asistenţa externă din 1961, amendaţii tu 1974 de L. 93 – 559 [22 USC 2420]. Această prevedere a fost modificată în 1985 prin adoptarea unei hotărâri privind scutirile acordate statelor Costa Rica, El Salvador şi Honduras.

8. O controversă referitoare la schimbul de informaţii secrete şi dat A acestea ar trebui considerate activităţi secrete s-a iscat în momentul în care Robert Gates a fost nominalizat pentru funcţia de Director al CIA, în 1991. Această dispută se referea la decizia luată la începutul anului 1980 de către administraţia Reagan de a transmite anumite informaţii secrete Irakului, ca sprijin în războiul împotriva Iranului. Gates a argumentat că acţiunea s-a desfăşurat în condiţiile unei relaţii tradiţionale bazate pe schimbul de

informaţii secrete. Oricum, senatorul Bill Bradley (D-NJ) a sugerat faptul că, din moment ce acţiunea nu afecta schimbul reciproc de informaţii, ci influenţa operaţiunile militare ale Irakului, se încadra în categoria activităţilor secrete şi, în consecinţă, ar fi trebuit raportată Congresului. Vezi US Senate, Select Committee on Intelligence, *Nomination of Robert Gates to Be Director of Centrul Intelligence*: *Hearings*, 102 d Cong., prima şedinţă, 1991, S. Hrg 102 – 799.1, 578 – 579, 945 – 950.

9. Pentru o trecere în revistă a operaţiunilor sovietice de infiltrare în guvernul Statelor Unite din anii ’30 şi 40, vezi John Earl Haynes şi Harvey Klehr, *Venona*: *Decoding Soviet Espionage în America* (Yale University Press, New Haven, Conn., 1999), capitolele 5 – 7, precum şi Herbert Romerstein şi Eric Breindel, *The Venona Secrets*: *Exposing Soviet Espionage and America’s Traitors* (Regnery, Washington, DC, 2000).

10. Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: HarperCollins, 1990; ediţia Harper-Perennial, 1991), 280-82, 334-37. In *The Venona Secrets*, 41-44, Romerstein şi Breindel susţin că White urma instrucţiunile sovietice in perioada anterioară atacului de la Pearl Harbor, atunci cand a recomandat adoptarea unei politici dure faţă de Japonia. (Uniunea Sovietică considera, la vremea respectivă, tensiunile dintre Statele Unite şi Japonia drept o garanţie impotriva unui atac japonez asupra părţii de est a Uniunii Sovietice.) Conform surselor de ştiri citate de Haynes şi Klehr, Henry Wallace,

vicepreşedinte in
timpul administraţiei Roosevelt intre anii 1941-1945, a remarcat că dacă ar fi
caştigat alegerile, l-ar fi nominalizat pe White in funcţia de ministru al finanţelor şi pe Laurence Duggan, care a fost, de asemenea, agent sovietic, in
funcţia de secretar de stat. Haynes and Klehr, *Venona*, 139 şi 411, nr. 49, şi
Christopher Andrew şi Vasili Mitrohin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 105, 109.

11. Andrew şi Gordievsky, *KGB*: *The Inside Story*, pp. 568 – 571.

12. Shultz şi Godson, *Dezinformatsia*, pp. 133 – 149, cuprinde o discuţie a cazului şi o analiză detaliată a conţinutului buletinului informativ.

13. Shultz şi Godson, *Dezinformatsia*, p. 38. Andrew şi Gordievsky susţin că Harry Hopkins, unul dintre consilierii de încredere ai Preşedintelui Franklin Roosevelt, se numără printre agenţii de influenţă care l-au ajutat să-şi menţină statutul „neutru” în ceea ce priveşte principalii aliaţi ai Americii în război, Marea Britanie şi Uniunea Sovietică. Gordievsky pretinde că a asistat la o prezentare susţinută de cel ce părea să-l controleze pe Hopkins în care era descris, în cel mai mic detaliu, rolul acestuia ca agent. Descrierea realizată de Gordievsky sugerează el Hopkins era manipulat, fără a-şi da seama, atât de Stalin, care îl linguşea ori de câte ori avea ocazia, cât şi de un ofiţer al serviciilor secrete sovietice, pretinzând a fi trimisul oficial al liderului sovietic. Andrew şi Gordievsky, *KGB*: *The Inside Story*, pp. 278, 334, 349 – 350. În schimb, Romerstein şi Breindel (*The Venona Secrets*, pp. 214 – 215) susţin că acele comunicaţii decriptate,

interceptate de sovietici, ce redau întâlnirile avute de Hopkins cu un *rezident* sovietic aflat în ilegalitate pe teritoriul Statelor Unite indică faptul că Hopkins era, de fapt, un agent rus manipulat.

14. Materialul citat face parte din lucrarea lui Bob Woodward, „CIA Currică Favor with Khomeini, Exiles", *The Washington Post*, 19 noiembrie 1986, p. Al, 28. Problema defectării a fost relatată în „Soviet Diplomat in Iran Defects and Flees to Britain", *The New York Times*, 24 octombrie 1982, p. A14.

15. Churchill relatează despre această tentativă în prezentarea celui de al Doilea Război Mondial. Acesta a încercat să eludeze suspiciunile lui Stalin trimiţând un mesaj „concis şi criptic" care nu reprezenta o avertizare în ceea ce priveşte atacul german. Acest mesaj făcea, pur şi simplu, referire la mişcările trupelor germane ce indicau un astfel de atac. Churchill spera că un asemenea mesaj „va capta atenţia lui Stalin şi îl va pune pe gânduri", ajungând, în final, singur la concluzia dorită. Din nefericire, aplicarea tacticii lui Churchill a fost, într-un fel, împiedicată de ambasadorul britanic la Moscova (*The Grand Alliance*, al treilea volum din seria *The Secret World War* [Houghton Mifflin, Hemliiti 1951], pp. 357 – 361). Gabriel Gorodetsky, *Grand Delusion*: *Stalin und the German Invasion of Russia* (Yale University Press, New Ilaven Connecticut, 1999), pp. 155 – 178, susţine că povestea este mult mai complicată decât sugerează Churchill.

16. Richard H. Schultz Jr., *The Secret War against Hanoi*: *Kennedy's and Johnson's Use of*

*Spies, Saboteurs, and Covert Warriors in North Vietnam* (HarperCollins, New York, 1999), pp. 130 – 148, 162 – 163. Schultz relatează că persoanele care coordonau programul au realizat, în cele din urmă, că acesta nu subminează încrederea nord-vietnamezilor. În absenţa unei mişcări de rezistenţă reale, vietnamezii din regiunea de Nord au ajuns, în timp, la ideea că alianţa era o farsă.

17. Ladislav Bittman, *The KGB and Soviet Disinformation*: *An Insider's View* (Pergamon-Brassey's, McLean, Va., 1985), pp. 112 – 113.

18. Andrew şi Mitrokhin, *The Sword and the Shield*, pp. 461 – 474.

19. Pentru relatarea lui Levchenko despre cariera sa în serviciile secrete urmată de dezertare, vezi John Barron, *KGB Today*: *The Hidden Hand* (Reader's Digest, New York, 1983; Berkley, New York, 1985), pp. 32 – 159.

20. Barron, *KGB Today*, pp. 76 – 81, 85 – 90, 93 – 94. Articolul, sugerând că operaţiunile desfăşurate în calitate de agent dublu erau o provocare a americanilor, urmărea reducerea sprijinului public pentru poziţia dui A adoptată de guvernul japonez împotriva presiunilor diplomatice sovietice Agentul GRU a fost, de fapt, eliberat. În schimb, scrisoarea urmărea crearea unor presiuni din partea publicului asupra guvernului japonez pentru a da curs unei cereri venite din partea sovieticilor; prin aceasta se solicita ca pilotul să fie readus în ţară. Dar scrisoarea nu şi-a atins scopul.

21. Tăinuirea totală nu este întotdeauna posibilă. Astfel, un serviciu secret străin poate

identifica locaţia de unde emite un post de radio „pirat” folosind echipamente de detectare a direcţiei. În orice caz, aceasta informaţie nu-i va fi accesibilă ascultătorului obişnuit.

22. G.J.A. O’Toole, *Honorable Treachery*: *A History of US Intelligence*, *Espionage*, *and Covert Action from the American Revolution to the CIA* (Atlantic Monthly, New York, 1991), pp. 236 – 239. Articolele apărute în *Providence Journal* erau de obicei versiuni uşor exagerate ale informaţiilor transmise de serviciile secrete. Efectul acestora era de a-i împiedica pe germani să afle că planul operaţiunilor lor fusese demascat, în mod similar, serviciile secrete britanice, acţionând clandestin, au făcut un efort imens pentru a determina întreaga Americă, înainte de intrarea acesteia în cel de-al Doilea Război Mondial, să susţină Marea Britanie şi să respingă politica de izolare. Potrivit unor relatări secrete despre istoria Marii Britanii, printre acţiunile desfăşurate de serviciile secrete britanice în Statele Unite se numărau şi inventarea unor eveni mente cu sprijinul anumitor jurnalişti, utilizarea unui post de radio din New York ca mijloc neavizat de propagandă, înfiinţarea unor grupări de faţadă şi hărţuirea unor figuri marcante ale opoziţiei, care făceau parte din Congres şi din mişcarea muncitorească americană. Vezi David Ignatius, „How Churchill’s Agents Secretly Manipulated the US before Pearl Harbor”, *The Washington Post*, 17 septembrie 1989, secţiunea „Outlook”, p. 1. Rămâne încă neclară măsura în care programul britanic nu era cunoscut de guvernul american şi, în special, de

preşedintele Roosevelt. Conform relatării lui Ignatius, în momentul în care istoria „secretă" a Marii Britanii a fost finalizată spre sfârşitul războiului, au fost înmânate copii ale acesteia atât lui Churchill, cât şi oficialilor serviciilor secrete britanice, dar şi lui Roosevelt. Pentru o relatare a acestui eveniment, vezi Thomas E. Mahl, *Desperate Deception*: *British Covert Action Operations in the United States, 1939 – 44* (Brassey's, Washington, DC, 1998). Printre acţiunile britanicilor mai erau incluse propaganda şi tot felul de „trucuri necinstite" al căror scop era înfrângerea lui Hamilton Fish, membru al Congresului şi susţinător al politicii de izolare (capitolul 6).

23. Într-un studiu al CIA, „Soviet Covert Action and Propaganda", este analizat fenomenul Vocea Naţională a Iranului, precum şi discursul acestui post de radio, care îndeamnă la sentimente antiamericane. Acest studiu a fost prezentat de către directorul adjunct pentru operaţiuni al CIA, pe data de 6 februarie 1980, în faţa Subcomisiei de Supraveghere, Comisia Permanentă a Serviciilor Secrete, Camera Reprezentanţilor. Studiul este reprodus în US House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, *Soviet Covert Action* (*The Forgery Offensive*): *Hearings*, Congresul al 96-lea, şedinţa a doua, 1980. Prezentarea apare la paginile 78 – 79.

24. Ray S. Cline, *The CIA*: *Reality vs. Myth*, ediţie revizuită (Acropolis, Washington, DC, 1982),

p. 151.

25. În urma confirmării publice de către senatorul Clifford Case a faptului că posturile de radio au beneficiat de fondurile acordate în secret de CIA, Congresul a decis în 1973 să sprijine, deschis, operaţiunile radio prin intermediul Comitetului International de Radiodifuziune. Acest comitet a fost constituit ca agenţie federală independentă. Cord Meyer, *Pacing Reality*: *From* World *Federalism to the CIA* (Harper and Row, New York, 1980), pp. 110 – 113.

26. Discursul a fost, de asemenea, publicat în New York Times, care l-a primit de la
Departamentul de Stat. Oricum, versiunea oferită mass-mediei străine includea
34 de paragrafe despre politica externă adoptată de sovietici, paragrafe care
lipseau din versiunea din New York Times. Datorită faptului că Uniunea Sovietică nu a contestat niciodată autenticitatea paragrafelor, John Ranelagh a concluzionat că acestea sunt veritabile (The Agency: The Rise and Decline of the CIA [New York: Simon şi Schuster, 1986], 287 n). Potrivit lui Ranelagh, CIA a primit două copii ale textului, o versiune completă (posibil de la o sursă din Uniunea Sovietică), precum şi o versiune corectată de la o sursă esteuropeană.
Explicaţia diferenţei dintre cele două versiuni ar fi protecţia sursei sovietice; versiunea completă a fost pusă numai la dispoziţia publicaţiilor nonamericane, pentru a masca legătura cu serviciile secrete americane. Pare destul de plauzibilă şi varianta conform căreia cele 34 de paragrafe suplimentare puse la dispoziţia mass-mediei străine, au fost scrise de experţi CIA în stilul lui Hruşciov; scopul lor era acela de a crea o stare de confuzie în ţările blocului
sovietic. Dacă este adevărat, motivul pentru care guvernul american a oferit publicaţiei New York Times numai versiunea autentică a discursului, a fost, probabil, acela de a se reduce posibilitatea ca opinia publică americană să fie indusă în eroare de către părţile fictive.

27. Jerrold L. Schecter şi Peter S. Deriabin, *The Spy Who Saved The World* (Scribner, New York, 1992), pp. 380 – 388.

28. Ignatius, „How Churchill's Agents

Secretly Manipulated the US before Pearl Harbor". Vezi Mahl, *Desperate Deception*, p. 34.

29. Pentru exemple şi discuţii referitoare la această tehnică şi la modul în care a fost utilizată de fosta Uniune Sovietică, vezi US House of Representatives, Permanent Select Committee on Intelligence, *Soviet Covert Action* (*The Forgery Offensive*), şi US Department of State *Soviet Influence Activities*: *A Report on Active Measures and Propaganda*, *1986 – 87*, august 1987, pp. 29 – 32, 79 – 80. A apărut o întrebare referitoare la o posibilă folosire a acestei tehnici de către SUA, făcându-se trimitere la faptul că CIA i-a adus la cunoştinţă lui Stalin conţinutul „discursului secret" a lui Hruşciov. Vezi *supra*, nota 26.

30. Termenul derivă din cuvântul rusesc *dezinformaţia*, care se referă la tehnica măsurilor active de a induce în eroare publicul astfel încât să acţioneze în interesul vorbitorului. Vezi Shultz şi Godson, *Dezinformatsia*, pp. 194 – 195.

31. Edwin Meese III, *With Reagan*: *The Inside Story* (Regnery Gateway, Washington, DC, 1992), pp. 170 – 171.

32. Susţinând, în faţa Curţii Constituţionale a Rusiei, scoaterea în afara legii în 1991 a Partidului Comunist, guvernul rus a pus la dispoziţia publicului o serie de documente din arhivele partidului, demonstrând că Departamentul de relaţii externe a sprijinit, în mod clandestin, de-a lungul anilor, aproximativ 100 de partide şi grupări politice în opt state.

Până în 1988, trei milioane de dolari au fost transferaţi în secret Partidului Comunist din

Statele Unite; în anii ’80, peste 20 de milioane de dolari au fost transferaţi aceluiaşi partid. Aceste fonduri le erau de obicei transmise beneficiarilor străini prin intermediul KGB. În anii ’20 şi 30, organizaţia comunistă Comintern a fost folosită în acest scop. Vezi Michael Dobbs, „Panhandling the Kremlin: How Gus Hall Got Millions”, *The Washington Post*, 1 martie 1992, p. Al, precum şi Harvey Klehr, John Earl Haynes şi Kiril Mikhailovich Anderson, *The Soviet World of* American *Communism* (Yale University Press, New Haven, Conn., 1998), capitolul 2.

33. Pentru o scurtă prezentare a acestui efort, vezi Sallie Pisani, *The CIA and the Marshall Plan* (University Press of Kansas, Lawrence, 1991).

34. Cline, *The CIA*, pp. 123 – 24.

35. Directiva Consiliului Naţional de Securitate 10/2 (iunie 1948), *apud* Cline, *The CIA*, p. 126.

36. US Senate, Church Committee, *Final Report*, vol. 1: *Foreign and Military Intelligence*, Congresul al 94-lea, şedinţa a doua, 1976, S. Rept. 94 – 755, 145.

37. Cline, *The CIA*, pp. 150 – 151.

38. Comisia Church, *Staff Report*: *Covert Action in Chile*: *1963 – 1973*, Congresul al 94-lea, prima şedinţă, 1975, Committee Print, 29, 45.

39. Comisia Church, *Staff Report*, 49 [subliniere în original].

40. Gregory F. Treverton, *Covert Action*: *The Limits of Intervention in the Postwar World* (Basic Books, New York, 1987), p. 142.

41. Treverton, *Covert Action*, p. 143.

42. La începutul Războiului Rece, CIA a organizat lovituri de stat în Iran (1953) şi Guatemala (1954). Kermit Roosevelt, *Countercoup*: *The Struggle for Control of Iran* (McGraw-Hill, New York, 1979); James Risen, „How a Plot Convulsed Iran in '53 (and in '79): A Secret CIA History", *The New York Times*, 16 aprilie 2000; Nick Cullather, *Secret History*: *The CIA's Classified Account of Its Operations in Guatemala, 1952 – 54* (Stanford University Press, Stanford, Calif., 2000); Richard H. Immerman, *The CIA in Guatemala* (University of Texas Press, Austin, 1982).

43. Pentru detalii referitoare la investigaţiile realizate de comisie, vezi Church Committee, *Alleged Assassination Plots Involving Foreign Leaders*: *Interim Report*, Congresul al 94-lea, prima şedinţă, 1975, S. Rept. 94 – 465.

44. Decretul 11905, „United States Foreign Intelligence Activities", 18 februarie 1976, secţiunea 5 (g) [41 Fed. Reg. 7733 (1976)].

45. Ordinul executiv 12036, 24 ianuarie 1978, secţiunea 2-305 [43 Fed. Reg. 3687 (1978)] şi Ordinul executiv 12333, 4 decembrie 1981, secţiunea 2.11 [48 Reg. Fed. 59947 (1981)]. Ambele prevederi renunţă la adjectivul "politic," dar înţelesul este, probabil, acelaşi.

46. În linii mari, trebuie să se stabilească dacă decretul care interzice asasinatele interzice şi operaţiunile care ar putea, din neatenţie, să aibă ca rezultat moartea unui lider politic sau (mai restrictiv) expunerea unei personalităţi politice la un risc semnificativ de a fi ucis.

47. Jules Witcover, *Sabotage al Black Tom*:

*Imperial Germany's Secret War in America, 1914 – 1917* (Algonquin, Chapel Hill, N.C., 1989).

48. Mărturia lui Stansfield Turner, în US House of Representatives, Permanen! Committee on Intelligence, Subcommittee on Legislation, *HR 1013, HR 1371, and Other Proposais which Address the Issue of Affording Prior Notice of Covert Actions to the Congress*: *Hearings*, Congresul al 100-lea, prima şedinţă, 1987, pp. 44 – 49.

49. Pentru o relatare recentă privind programul de asistenţă acordaţii mujahedinilor de către o persoană implicată în conducerea unei reţele, vezi Mohammad Yousaf şi Mark Adkin, *The Bear Trap*: *Afghanistan's Untold Story* (Leo Cooper, Londra, 1992). Yousaf a fost liderul departamentului pentru Afganistan al Serviciului secret pakistanez la mijlocul anilor '80.

50. Sefton Delmer, *Black Boomerang* (Viking, New York, 1962), p. 120.

51. Menţionăm că legea din 1991 (PL 102 – 88) care defineşte acţiunile secrete se referă la activităţi „în care rolul guvernului Statelor Unite nu va fi evident sau nu va fi *recunoscut în mod public*" [sublinierea noastră]. Este vorba despre cazurile în care rolul guvernului, deşi evident pentru un observator al situaţiei internaţionale, chiar relatate în presă, nu este recunoscut în mod public.

52. Vezi discuţia referitoare la acest incident prezentată în capitolul 3.

53. Pentru o opinie favorabilă statutului acţiunilor secrete aflate sub incidenţa legilor

internaţionale, vezi W. Michael Reisman şi James E. Baker, *Regulating Covert Action*: *Practices, Contexts, and Policies of Covert Coercion Abroad* în *International and American Law* (Yale University Press, New Haven, Conn., 1992). În general, Reisman şi Baker susţin că practica actuală a statelor, precum şi reacţia lor şi a comunităţii internaţionale implică faptul că multe acţiuni secrete nu sunt neapărat ilegale din perspectiva legislaţiei internaţionale. Oricum, cei doi interpretează destul de strict principiul nonintervenţiei din Carta Naţiunilor Unite şi mult mai permisiv noţiuni-cheie precum „activităţi secrete", „lege" şi „practică acceptată".

54. Nikita S. Hruşciov, *Khrushchev remembers*: *The Last Testament* (Little, Brown, Boston, 1974), pp. 447 – 448.

55. Vezi lucrarea lui John Dyson, *Sink the Rainbow! An Enquiry into the "Greenpeace Affair"* (Londra: Gollancz, 1986), 157-86, pentru o relatare a modului în care guvernului francez a gestionat acest episod.

56. Secţiunea 662(a) a Legii privind asistenţa externă din anul 1961, amendată. Amendamentul Hughes-Ryan a fost abrogat oficial odată cu punerea în aplicare a Legii privind autorizarea activităţii serviciilor secrete pentru anul fiscal 1991. Nouă lege păstra condiţia avizării de către preşedinte şi includea, de asemenea, cazul operaţiunilor secrete derulate nu numai de CIA, ci de toate agenţiile guvernamentale ale Statelor Unite. Legea dispunea ca toate hotărârile să fie "în scris". În cazul în care trebuie acţionat imediat, dar nu există timpul necesar pentru a emite o hotărâre scrisă, preşedintele este totuşi obligat să emită o astfel de hotărâre "în cel mult 48 de ore de la adoptarea deciziei" pentru autorizarea acţiunii.

57. Comisia Church a ignorat, în *Raportul Final*, chestiunea

“negării plauzibile” în ceea ce priveşte efectele amendamentului. În schimb, în raport sunt prezentate cele două rezultate ale amendamentului, şi anume (1) responsabilitatea statutară a Executivului de a informa Congresul despre acţiunile secrete, şi (2) includerea comisiilor de politică externă ale Senatului şi Camerei Reprezentanţilor printre comisiile care trebuie informate. Volumul 1: *Foreign*
*and Military Intelligence*, 151.

58. *Report of the Congressional Committees Investigating the Iran Cont ni Affair*, Congresul al 100-lea, prima şedinţă, 1987, H. Rept. 100.433, S, Rept. 100 – 216, 271.

59. „Iraq Liberation Act of 1998”, L. 105 – 338, 31 octombrie 1998. Mlaura a fost adoptată ca urmare a rapoartelor referitoare la acţiunile secrete nereuşite ce aveau ca scop înlăturarea lui Saddam Hussein de la putere. Don Oberdorfer, „A Covert Plan to Oust Hussein”, *Washington Post Weekly Edition*, 25 – 31 ianuarie 1993, p. 19, şi Jim Hoagland, „How CIA’s Secret War on Saddam Collapsed”, *Washington Post*, 26 iunie 1997, p. A21. Vezi şi Marie Colvin, „Revealed: CIAS Bungled Iraqi Coup”, *The Sunday Times* (Londra), 2 aprilie 2000.

60. David Lowe, „Ideea to Reality: A Brief History of the National Endowment for Democracy”, oferă o relatare despre istoria legislativă a înfiinţării NED. Disponibil pe www.ned.org/about/about.html.

61. Spre exemplu, Fundaţia Konrad Adenauer (Stiftung) asociată cu Partidul Creştin-Democrat, conform propriilor afirmaţii, a colaborat, „mai mult de 30 de ani, cu parteneri din întreaga lume… Aceste acţiuni internaţionale… sunt finanţate de Ministerul German Federal pentru

Cooperare şi Dezvoltare Economică, Ministerul de Externe... Printre partenerii străini se numără partide politice, parlamente şi guverne; institute de educaţie şi cercetare; universităţi; confederaţii şi sindicate din industrie; cooperative; organizaţii feministe, de mediu şi de automotivare; şi mass-media. Toate aceste proiecte au ca scop promovarea democraţiei şi dezvoltarea, îmbunătăţirea relaţiilor interumane, indiferent de etnie, sprijinirea organizaţiilor de automotivare şi combaterea cauzelor sărăciei şi distrugerii mediului" [citat pe www.kas.de/stiftung/englisch/international.html.].

62. Christopher Andrew, *Her Majesty's Secret Service*: *The Making of thp British Intelligence Community* (Viking, New York, 1986), pp. 476 – 477 S-a sugerat că înfiinţarea SOE ca agenţie separată de MI6 s-a datorat, tu parte, argumentelor politice interne. Plasând SOE în subordinea ministrului Economiei, membru al Partidului Laburist, Churchill răspuns solicitărilor partenerilor să-i de coaliţie, în sensul împărţirii controlului asupra sor viciilor secrete. M.R.D. Foot, *SOE*: *An Outline History of the Special Oper*ations *Executive*, *1940 – 46*, ediţie revizuită (University Publication» of America, f.l., 1986), pp. 19 – 20.

63. Church Committee, *Final Report*, vol. 1, 106. Vezi şi Arthur B. Darling, *The Central Intelligence Agency*: *An Instrument of Government*, *to 1950* (Pennsylvania State University Press, University Park, 1990), pp, 245 – 281. (Darling a fost istoric în cadrul CIA din 1952

până în 1954; iniţial secretă, istoria lui Darling a fost publicată în 1989, în colaborare cu Departamentul de cercetare istorică al Agenţiei.)

64. Mai târziu, denumirea a fost schimbată în Direcţia de Operaţiuni (Directorate of Operations – DDO).

65. Church Committee, *Final Report*, vol. 1, pp. 107 – 108.

66. Pentru o opinie critică referitoare la componentele activităţii de informaţii, vezi Kenneth G. Robertson, „The Study of Intelligence in the United States", în Roy Godson (ed.), *Comparing Foreign Intelligence*: *The U.S.*, *the USSR*, *the UK and the Third World* (Pergamon-Brassey's, McLean, Virginia, 1988), pp. 26 – 28.

67. George Kennan, oficial al Departamentului de Stat, care a contribuit la stabilirea normelor operaţionale iniţiale ale OPC, a afirmat că acţiunile secrete au fost un instrument folosit în politica externă. În consecinţă, aceste acţiuni secrete intrau exclusiv în responsabilitatea Departamentului de Stat şi a instituţiilor militare naţionale. Datorită anumitor caracteristici, OPC putea fi considerată parte a CIA, dar strategia şi orientarea erau impuse de către Departamentul de Stat şi organele puterii de stat. Astfel, pe timp de pace, secretarul de stat era cel care îl numea pe liderul OPC şi îi supraveghea activităţile. Darling, *The Central Intelligence Agency*, p. 277.

## Capitolul 5. Spion contra spion: activitatea de contrainformaţii

1. Termenul contraspionaj poate fi definit ca fiind o formă de protecţie împotriva
“sabotajului sau asasinatelor comise de către sau în numele unor puteri,
organizaţii sau persoane străine, sau împotriva activităţilor de terorism internaţional.” (Citatul face parte din definiţia contraspionajului prezentată în
Ordinul executiv 12333 al preşedintelui Reagan din 4 decembrie 1981, “United
States Intelligence Activities,” paragraful 3.4[a].) Aceasta poate fi considerată
o definiţie potrivită, din moment ce aceste acţiuni sunt identice sau similare cu
acţiunile secrete desfăşurate de un serviciu secret al unui stat inamic; protecţia
împotriva acestora poate implica, aşadar, multe dintre metodele folosite
împotriva acţiunilor serviciilor secrete ale statelor duşmane.

2. Definiţia contraspionajului din decretul la care ne-am referit în cadrul notei 1 exclude „programele de securitate a comunicaţiilor, documentelor şi personalului”. Astfel, este reflectat faptul că, în general, ministerele şi agenţiile americane care lucrează cu informaţii secrete sunt responsabile pentru programele de securitate, pentru a proteja acele informaţii, în timp ce principala responsabilitate a FBI ŞI CIA se referă la acţiunile de contraspionaj (ţinând cont de definiţia din decret), desfăşurate atât în ţară, cât şi în străinătate. Oricum, din punctul nostru de vedere, securitatea ar trebui considerată parte a contraspionajului, din moment ce ambele îndeplinesc aceeaşi funcţie.

3. Harold C. Relyea, „The Presidency and the People’s Right to Know”, în Harold C. Relyea (ed.), *The Presidency and Information Policy* (Center for the Study of the Presidency, New York, 1981), pp.

11 – 19.

4. "Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departaments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States", Decretul 10290, 24 septembrie 1951.

5. Decretul 12958, „Classified National Security Information", 17 aprilie 1995. Biroul pentru supravegherea securităţii informaţiilor (Information Security Oversight Office – ISOO) este responsabil cu supravegherea programului guvernamental de securitate a informaţiilor clasificate. Raportul anual al ISSO oferă o scurtă trecere în revistă a programului de clasificare şi declasificare a informaţiilor. Potrivit celui mai recent raport, 3.846 de oficiali guvernamentali au deţinut dreptul de clasificare a informaţiilor; în decursul anului, s-au luat mai mult de opt milioane de decizii de clasificare a documentelor. Dintre acestea, 44% aparţin CIA; 27%, Departamentul Apărării; Biroului Naţional de Recunoaştere, 24%; Departamentul Justiţiei, 2%, Departamentului de Stat, 2%; celorlalte agenţii, 1%. (Aproape 127 de milioane de pagini ale unor materiale clasificate în trecut au fost declasificate.) ISOO, *FYI999 Report to the President*, 15 august 2000. Rapoartele anuale ale ISOO sunt disponibile la adresa www.fas.org/zgp/isoo/index.html.

6. Decretul 12958, secţiunea 1.3.

7. Legea securităţii naţionale emisă în anul 1947, secţiunea 102 (d) (3) M USC 403 (d) (3)].

Decretul 12958, secţiunea 4.4, îi autorizează" pe directorul CIA, precum şi pe miniştrii de Externe, al Apărării şi al Industriei Energetice să creeze programe speciale de acces.

8. Decretul 12958, secţiunea 4.4(a) şi (b) (3). Echipa de supraveghere este condusă de directorul Biroului pentru supravegherea securităţii informaţiilor, care este responsabil pentru sistemul de clasificare a informaţiilor referitoare la siguranţa naţională.

9. Decretul 12958 defineşte „nevoia de a şti" drept „stabilirea de către deţinătorul unor informaţii clasificate a faptului că un potenţial beneficiar are nevoie de acces... pentru a-şi îndeplini, în mod legal l autorizat, toate atribuţiile funcţiei sale guvernamentale" (secţiunea 4. l[c).

10. *Keeping the Nation's Secrets*: *A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices*, 23 noiembrie 1985, *apud* US Senate, Select Committee on Intelligence *Meeting the Espionage Challenge*: *A Review of United States Counterintelligence and Security Programs*, Congresul al 99-lea, şedinţa a doua, 1986, S. Rept. 99 – 522, p. 66.

11. Până în 1989, Uniunea Sovietică a dat publicităţii o singură cifră, despre care a spus că reprezintă bugetul pentru apărare. Totuşi, cifra era, în mod evident, mult prea mică pentru a include toate cheltuielile militare sovietice. În 1989, când au făcut publică o valoare totală mult mai mare a cheltuielilor pentru apărare, sovieticii au explicat că cifra publicată anterior includea

numai salariile şi normele de întreţinere ale membrilor forţelor armate. În mod similar, Republica Populară Chineză a publicat o cifră despre care pretindea că reprezintă cheltuielile pentru apărare; şi această cifră era, de asemenea, mult prea mică, dar nu se ştie ce componentă a cheltuielilor de apărare includea, de fapt, dacă cifra reprezenta, într-adevăr, ceva.

12. *Keeping the Nation's Secrets*, p. 49.

13. Pentru o analiză mai detaliată a sistemului menţinerii secretului oficial în Marea Britanie, care este comparat, în linii mari, cu cel din Suedia şi Statele Unite, vezi K.G. Robertson, *Public Secrets*: *A Study in the Development of Government Secrecy* (St. Martin's, New York, 1982). De la publicarea studiului lui Robertson, Marea Britanie a adoptat două legi referitoare la păstrarea secretului guvernamental: un amendament (în 1989) la Legea secretelor oficiale şi o Lege a dreptului la liberă informare (în 2000). Pentru o analiză a Legii secretelor oficiale şi a amendamentului din 1989, vezi Rosamund Thomas, *Espionage and Secrecy*: *The Official Secrets Acts 1911 – 1989 of the United Kingdom* (Routledge, New York, 1991). Textul Legii dreptului la liberă informare este disponibil la http://www.legislation.hmso.gov.uk/acts/acts2000/20000036.htm

14. În 1997, o comisie înfiinţată pentru a analiza programele guvernamentale de clasificare a informaţiilor secrete a susţinut faptul că „sistemul de clasificare... este folosit prea des pentru a nega dreptul populaţiei de a înţelege procesul de luare a deciziilor politice" şi „cea mai

bună metodă de a asigura păstrarea secretelor, mai ales a celor importante, care trebuie *să rămână* secrete, este ca secretizarea să revină la rolul său limitat, dar necesar. Secretele pot fi păstrate într-un mod mult mai eficient dacă se renunţă la tăinuirea lor". *Secrecy*: *Report of the Commission on Protecting and Reducing Government Secrecy* (Government Printing Office, Washington, DC, 1997), p. XXI [subliniere în original], www.access. gpo. gov/int.

15. Decretul 12958 menţionează faptul că „informaţiile secrete nu vor fi, în niciun caz, clasificate doar pentru ca o persoană, organizaţie sau agenţie să nu fie pusă într-o lumină proastă" (secţiunea 1.8[al [2]). Există totuşi posibilitatea ca informaţiile să fie în continuare clasificate pentru ca guvernul să nu fie pus într-o lumină proastă. Acest lucru este subliniat de faptul că „informaţiile care ar putea afecta relaţiile dintre Statele Unite şi un guvern străin" nu sunt declasificate în mod automat (secţiunea3.4[b][6]).

16. Bob Woodward, „CIA Paul Millions to Jordan's King Hussein", *Washington Post*, 18 februarie 1977, p. A1.

17. Legea energiei atomice din 1954, secţiunea 11 y [42 USC 2014 y].

18. Secţiunea 148 [42 USC 2168].

19. Adm. B.R. Inman, „National Security and Tehnical Information", lucrare prezentată în cadrul întrunirii anuale a American Society for the Advancement of Science, ianuarie 1982, Washington, DC.

20. US Senate, Committee on Commerce,

Science and Transportation *Statement of Louis J. Freeh, Director, FBI, on July 25.1996, Regarding „Impact of Encryption on Law Enforcement and Public Safety”*, http://www.fas.org./irp/congress/1996_hr/s960725f.htm

21. S-a sugerat ca toţi producătorii de programe de criptare să asigure un *escrow key* – adică informaţiile care să permită o decriptare cât mai rapidă. Astfel, o agenţie de aplicare a legii ar putea folosi această cheie pentru a citi materialele interceptate sau informaţiile dintr-un calculator, toate acestea realizându-se pe baza unui mandat de percheziţie. Potrivit lui Freeh, directorul FBI, tipurile speciale de criptare disponibile pe piaţă “pot afecta echilibrul legal şi aşa delicat asigurat prin cel de-al Patrulea Amendament al Constituţiei S.U.A., din moment ce, atunci când un judecător emite un mandat de percheziţie, mandatul nu va avea nicio valoare practică în cazul unei astfel de criptări” (declaraţia lui Freeh).
Potrivit lui Freeh, criptarea ce utilizează “escrow key” ar putea contribui la restabilirea echilibrului legal, însă acest argument nu s-a bucurat de sprijin.

22. Pe 12 ianuarie 2000, Ministerul Comerţului din Statele Unite a emis o serie de norme care permiteau, în mare măsură, exportul neîngrădit al unor programe de criptare foarte avansate. Declarana de presă a Ministerului Comerţului este disponibilă la adresa http://www.fas.org/irp/news/2000/01/000113-crypto-bxa.htm

23. În Statele Unite, cel puţin la nivel teoretic, lipsa de loialitate faţă de guvern nu-i permite nici unei persoane să deţină o funcţie în serviciile publice federale; totuşi, s-a renunţat la acest criteriu în cazul posturilor care nu solicită

acces ia informaţiile clasificate. Vezi Guenter Lewy, „The Federal Loyalty-Security Program”, în Roy Godson (ed.), *Intelligence Requirements for the 1980's*: *Domestic Intelligence* (Lexington, Lexington, Mass., 1986), p. 147 *passim*, pentru o analiză a acestei evoluţii. Aspectul loialităţii este prezentat în Decretul 10450 al preşedintelui Truman, „Security Requirements for Government Employment”, 27 aprilie 1953.

24. Cu condiţia ca această convingere să nu fi stat la baza nici unei acţiuni violente sau criminale. Chiar şi în acest caz, nu ar fi fost admisibilă întocmirea unei liste complete cu membrii organizaţiei, cu excepţia cazului în care nu se putea demonstra că erau implicaţi în acţiunile violente ale organizaţiei. Aceste aspecte sunt analizate în capitolul următor.

25. US Senate, Subcommittee on Criminal Laws and Procédures, Committee on the Judiciary *Hearings on the Erosion of Law Enforcement Intelligence and Its Impact on the Public Security*, partea a opta, Congresul al 95-lea, şedinţa a doua, 1978, *apud* Guenter Lewy, „The Federal Loyalty – Security Program”, p. 152.

26. În 1983, Biroul de Evaluare a Tehnologiei (Office of Technology Assessment – OTA) al Congresului Statelor Unite a elaborat un studiu critic la adresa reclamaţiilor întemeiate pe rezultatele testului poligraf. *Scientific Validity of Polygraph Testing*: *A Research Review and Evaluation – Tehnical Memorandum*, OTA-TM-H-15 (Government Printing Office, Washington, DC, 1983). În anul următor, Departamentul Apărării, a

cărui Agenţie Naţională de Securitate foloseşte poligraful, a publicat un studiu care îl combătea pe cel dintâi. US Departament of Defense, *The Accuracy and Utility of Polygraph Testing* (Government Printing Office, Washington, DC, 1984).

27. Vezi analiza din cadrul acestui capitol a operaţiunii cubaneze de inducere în eroare, derulată împotriva Statelor Unite. Cel puţin doi dintre aceşti agenţi dubli, pe care comunitatea serviciilor secrete îi considera loiali, au fost supuşi unor teste cu poligraful.

28. Aceste teste poligraf sunt analizate în US Senate, Select Committee on Intelligence, *An Assessment of the Aldrich H. Arnes Espionage Case and Its Implications for U.S. Intelligence*, 1 noiembrie 1994, pp. 32 – 34, 71 – 74. Potrivit FBI, analiza din iunie 1993 a rezultatelor testelor poligrafice realizate în 1986 de către experţii instituţiei a demonstrat faptul că Ames minţise; oricum, până la momentul efectuării acestei reexaminări, Ames făcea deja obiectul unor „anchete serioase” (p. 82). Este aşadar dificil de ştiut în ce măsură următoarea analiză a rezultatelor testelor poligraf a fost afectată de faptul că existau multe alte motive de suspiciune.

29. Pentru activitatea serviciilor secrete, pentru o trecere în revistă a cazurilor dintre 1980 şi 1986, vezi *Meeting the Espionage Challenge*, pp. 12 – 15, US Senate, Select Committee on Intelligence. Pentru o listă a cazurilor de după această perioadă, vezi Defense Security Service, *Recent Espionage Cases, 1975 – 1999: Summaries*

*and Sources*, Security Research Center (septembrie 1999), http://www.dss.mil/training/pub.htm

30. Spre exemplu, un subofiţer din cadrul armatei care a vândut informaţii strict secrete obţinute din interceptarea comunicaţiilor Uniunii Sovietice şi statelor semnatare ale Pactului de la Varşovia, vreme de şase ani, i-a spus unui agent sub acoperire al FBI următoarele: „Nu aveam probleme cu banii. Am hotărât doar că nu mai vreau ca niciodată să mă gândesc de unde voi face rost de următorul dolar. Nu sunt împotriva Americii. Preţuiesc steagul la fel de mult ca oricare altă persoană”. Defense Security Service, *Recent Espionage Cases*, p. 22.

31. Totuşi, se pare că Hanssen nu fusese motivat nici de lăcomie. El susţine, într-un mesaj, că a început să admire serviciile secrete sovietice la vârsta de 14 ani, în momentul în care a citit memoriile lui Kim Philby; este total lipsit de sens, din moment ce Hanssen s-a născut în 1944, iar cartea lui Philby a fost publicată abia în anul 1960. Acest mesaj este citat în depoziţia guvernului Statelor Unite ale Americii în favoarea arestării şi emiterii unor mandate de percheziţie împotriva lui Hanssen, depusă la dosar la US District Court din Virginia de Est. (Potrivit altor mesaje citate în depoziţie, Hanssen nu pare a fi foarte îngrijorat când e vorba de bani, deşi acesta solicită o sumă iniţială de o sută de mii de dolari.) Depoziţia este disponibilă pe http://www.fas.org/irp/ops/ci/hanssen_affidavit.html

32. După cum se menţionează într-un raport al Comisiei senatoriale pentru activitatea serviciilor secrete, „ameninţarea venită din partea

altor servicii secrete ostile la adresa sistemelor informaţionale americane este amplificată de creşterea surprinzătoare a numărului şi performanţelor computerelor, precum şi a volumului de informaţii stocate în acestea... Computerele sporesc foarte mult numărul informaţiilor ia care poate avea acces o persoană". (*Meeting the Espionage Challenge*, pp. 35 – 36.) Pentru o relatare documentată a problemelor specifice sistemelor computerizate de securitate, precum şi a cazurilor de spiona) în domeniu, vezi Clifford Stoll, *The Cuckoo's Egg*: *Tracking a Spy through the Maze of Computer Espionage* (Doubleday, New York, 1989)

33. Pentru un exemplu, vezi *supra*, capitolului 2, nota 70.

34. US Senate, Select Committee on Intelligence, *Meeting the Espionage Challenge*, pp. 34 – 35.

35. După cum afirma în anul 1987 James Schlesinger, fost secretar de stat al Apărării, „în ultimii ani, sovieticii ne urmăreau îndeaproape, astfel încât am putut să detectăm şi să înlăturăm infiltrările... în momentul de faţă, ne confruntăm cu un progres al tehnologiei sovietice, care totuşi nu este mai avansată decât tehnologia noastră; într-adevăr, în anumite domenii au fost cu un pas înaintea noastră... Avem multe de învăţat de la sovietici, atât în ceea ce priveşte construirea ambasadelor, cât şi cu privire la derularea anumitor operaţiuni. Sovieticii s-au gândit îndelung la crearea unor sisteme de securitate speciale pentru ambasade, precum şi la

construirea acestora”. Mărturia lui James Schlesinger în faţa Comisiei Senatoriale pentru Buget, *apud* „For the Record”, *The Washington Post*, 1 iulie 1987, p. A18.

36. Christopher Andrew şi Oleg Gordievsky, *KGB*: *The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (HarperCollins, New York, 1990; ediţia Harper-Perennial, 1991), pp. 296 – 298, 598 – 599.

37. După cum am menţionat deja, Howard a reuşit să se sustragă supravegherii FBI şi, câteva luni mai târziu, a fost văzut la Moscova. Iurcenko a revenit în Uniunea Sovietică, fapt ce sugerează că este posibil ca actul sau iniţial de trădare să fi fost o înscenare, iar el să fi fost trimis de sovietici pentru a induce în eroare serviciile secrete americane sau din alt motiv. Dacă aceasta este situaţia, pentru a întări autenticitatea faptelor lui Iurcenko sau buna sa credinţă s-a renunţat la Pelton şi la Howard – care nu mai erau angajaţi de SUA sau nu le mai erau de niciun folos sovieticilor. Vezi David Wise, *The Spy Who Got Away*: *The Inside Story of Edward Lee Howard* (Random House, New York, 1988), pp. 17 – 21 *passim*.

38. Pentru o discuţie despre „Tricycle” (tricicletă) (un iugoslav pe nume Dusko Popov) şi despre modul de utilizare al chestionarului, vezi B. Bruce Briggs, „Another Râde on Tricycle”, *Intelligence and National Security*, 7, nr. 2 (aprilie 1992), pp. 77 – 100. Este de remarcat faptul că acest chestionar a ajuns în mâinile americanilor odată cu mesajul japonez despre un „atac cu bombă” din septembrie 1941. În acest mesaj

interceptat se solicita consulatului japonez din Honolulu să indice cu exactitate care sunt cabinele navelor americane de la Pearl Harbor. Mesajul a fost decodificat, dar se pare că nimeni nu s-a întrebat de ce aveau japonezii nevoie de informaţii atât de detaliate. Vezi Gordon W. Prange, *At Dawn We Slept*: *The Uniold Story of Pearl Harbor* (McGraw-Hill, New York, 1981), pp. 248 – 252.

39. Pentru detalii despre agentul american dublu cu activitatea cea mai îndelungată din timpul Războiului Rece, vezi David Wise, *Cassidy's Run*: *The Secret Spy War over Nerve Gas* (Random House, New York, 2000), povestea unui sergent major din armata americană, Joseph Cassidy, care a fost „fluturat" prin faţa serviciilor secrete sovietice şi care a lucrat ca agent dublu peste 20 ani. Potrivit lui Wise, în urma acestei activităţi au fost demascaţi doisprezece ofiţeri ruşi, au apărut trei „emigranţi ilegali" şi un „cod Armaghedon" utilizat de serviciile secrete ruse. În această perioadă, Cassidy a furnizat peste 4.500 de pagini de documente clasificate ruşilor, inclusiv „informaţii" menite să îi inducă în eroare pe sovietici cu privire la succesul înregistrat de americani în încercările lor de obţinere a armelor chimice. Unul dintre scopurile americanilor a fost să îi determine pe ruşi să cheltuiască timp şi resurse pe o formulă despre care oamenii de ştiinţă americani stabiliseră deja că nu este eficientă (pp. 63 – 69). Wise bănuieşte că înşelăciunea s-a întors împotriva lor atunci când sovieticii au reuşit să depăşească obstacolele care

îi blocaseră pe americani şi au produs o nouă substanţă chimică letală; cu toate acestea, dovezile în favoarea acestei opinii sunt circumstanţiale şi nu foarte convingătoare (pp. 63 – 69).

40. John C. Masterman, *The Double-Cross System* in the *War of 1939 to 1945* (Yale University Press, New Haven, Connecticut, 1972), p. 3. Această lucrare, elaborată de cel care a condus sistemul, este sursa relatării din text; pentru mai multe detalii, vezi pp. 30 – 31, 38 – 40, 41, 49, 58.

41. Agentul care lucrase iniţial pentru serviciul militar de informaţii german (Abwehr) la sfârşitul anilor ’30; britanicii care ştiau de existenţa lui i-au permis să îşi continue activitatea în parte şi pentru că acesta colabora cu MI6, ceea ce ar fi complicat eforturile de a-l urmări în justiţie.

42. Chiar şi după ce aliaţii au debarcat în Normandia în data de 6 iunie, agenţii dubli britanici şi-au continuat activitatea. De exemplu, pe data de 9 iunie, „Garbo” (nume de cod pentru Juan Pujol, unul dintre cei mai de succes agenţi dubli ai MI5) a transmis prin radio la Berlin ştirea că invazia din Normandia era o diversiune menită să atragă rezervele germane şi să slăbească forţele care protejau portul Calais, unde urma să aibă loc adevăratul atac. La primirea acestui mesaj, înaltul Comandament german a contramandat ordinul dat anterior privind un contraatac german asupra forţelor aliate pe plaja din Normandia. Drept mulţumire pentru

„informaţia” furnizată de Pujol, Hitler i-a conferit Crucea de Fier. Christopher Andrew, *Her Majesty*'s *Secret Service*; *The Making of the British Intelligence Community* (Viking, New York. 1986), p. 488. Pentru informaţii privind viaţa lui Pujol ca dublu agent britanic, vezi Juan Pujol şi Nigel West, *Garbo* (Weidenfeld şi Nicolson, Londra, 1985).

43. Michael Wines şi Ronald J. Ostrow, „Cuban Defector Claims Double Agents Duped U.S.”, *Washington Post*, 12 august, 1987, p. A8.

44. Potrivit unui important membru al minorităţilor din Comisia permanentă privind activitatea serviciilor de informaţii, din Camera Reprezentanţilor, s-a descoperit că „aproape toţi agenţii est-germani” recrutaţi de ame ricani erau „agenţi dubli”. Bud Shuster, „HiTech vs. Human Spying”, *The Washington Times*, 11 februarie 1992, p. F3.

45. Directorul NSA, gen. – lt. Michael V. Hayden, USAF, a descris în felul următor principalele provocări pe care le-a înfruntat agenţia sa: „Mijloacele de comunicaţii ale adversarului nostru sunt influenţate de ciclul de dezvoltare al industriei globale care se mişcă cu viteza luminii […]… telefoane celulare, mijloace de criptare, *comunicaţii prin intermediul fibrei optice*, comunicaţii digitale”. Dan Verton, „NSA Warns It Can’t Keep Up with Rapid Changes in IT”, Infoworld.com, 19 februarie 2001 [sublinierea noastră].

46. Pentru două discuţii generale despre problema tacticii militare de dezinformare, vezi

Donald Daniel şi Katherine Herbig (ed.), *Strategic Military Deception* (Pergamon, New York, 1982), precum şi John Gooch şi Arnos Perlmutter, *Military Deception* and Strategic Surprise (Frank Cass, Londra, 1982).

47. Pentru tacticile de dezinformare folosite înainte şi în timpul celui de-al Doilea Război Mondial, vezi: Michael Howard, *British Intelligence in the Second World War*: *Strategie Deception* (Her Majesty's Stationery Office, Londra, 1990); Michael Mihalka, *German Strategie Deception* in the *1930 s*, Rand Note N-1557-NA (RAND, Santa Monica, Calif., 1980); Barton Whaley, „Covert Rearmament in Germany 1919 – 1939: Deception and Misperception", *Journal of Strategic Studies*, nr. 5 (martie 1982), pp. 3 – 39; Barton Whaley, *Codeword Barbarossa* (MIT, Cambridge, Mass., 1973); David M. Glantz, *Soviet Military Deception* in the *Second World War* (Frank Cass, Londra, 1989); Charles Cruickshank, *Deception in World War* II (Oxford University Press, Oxford, 1979); Michael Handel (ed.), *Strategic and Operational Deception in the Second World War* (Frank Cass, Londra, 1987); şi o ediţie specială a *Intelligence and National Security*, *2*, nr. 3 (iulie 1987).

48. „CEKA" este un acronim bazat pe al doilea şi al treilea cuvânt din denumirea în limba rusă a Comisiei ruse extraordinare de combatere a contrarevoluţiei şi a sabotajului.

49. Pentru o discuţie despre Trust, vezi John J. Dziak, *Chekisty: A History of the KGB* (Lexington, Massachusetts: Heath, Lexington,

1988), 47 – 50 şi Andrew şi Gordievsky, *KGB: The Inside Story,* 97 – 106.

În mod similar, serviciile de informaţii sovietice şi cele poloneze după al Doilea Război Mondial utilizând un agent polonez dublu au reuşit să fi convingă pe britanici şi pe americani că un grup de rezistenţă polonez (Wolność i Niepodległość, WIN) era încă activ şi necesita asistenţă secretă; de fapt, WIN era controlat de KGB şi de serviciile de informaţii poloneze. Până în 1952, când polonezii şi sovieticii au recunoscut activitatea de dezinformare, serviciul secret polonez s-a folosit de WIN pentru a descoperi ultimii membri activi ai rezistenţei anticomuniste din Polonia şi pentru a transmite informaţii eronate despre situaţia internă din Polonia în Occident. Dziak, *Chekisty,* 123 – 24.

50. John Prados, *The Soviet Estimate*: *US Intelligence Analysis and Russian Military Strength* (Dial, New York, 1982), pp. 42 – 43.

51. Pentru o discuţie pe larg despre aceste declaraţii exagerate şi scopul lor, vezi Arnold L. Horelic şi Myron Rush, *Strategic Power and Soviet Foreign Policy* (University of Chicago Press, Chicago, 1966), pp. 42 – 116.

52. Horelick şi Rush, *Strategic Power*, pp. 117 – 140.

53. Prange, *At Dawn We Slept*, pp. 338, 353.

54. Trebuie să ţinem, de asemenea, cont de modul în care adversarul procesează informaţiile. Dacă, de exemplu, din cauza timpului scurt avut la dispoziţie, nu se vor putea analiza pe îndelete fotografiile înainte de a se lua o decizie, atunci

poate fi indus în eroare printr-o imitaţie de calitate inferioară. Până când o analiză detaliată îi va fi indicat adversarului faptul că obiectivul este unul fals, acesta va fi acţionat deja pe baza primei impresii greşite. Iată alt motiv pentru care operaţiunile de dezinformare sunt utilizate mai des pe timp de război decât pe timp de pace.

55. Howard, *British Intelligence in the Second* World *War*: *Strategic Deception*, p. 224.

56. HJ. Giskes, *London Calling North Pole* (William Kimber, Londra, 1953), şi M.R.D. Foot, *SOE*: *An Outline History of the Special Operations Executive*, *1940 – 46*, ediţie revăzută (University Publications of America, Frederick, Dr., 1986), pp. 130 – 134. Giskes era ofiţerul german de contrainformaţii care conducea operaţiunea. Se pare că germanii nu au folosit acest canal pentru a-i induce în eroare pe britanici privind alte activităţi decât cele ale agenţilor lor SOE din Olanda.

57. Acest incident este relatat în H.M.G. Lauwers, „Epilogue”, în Giskes, *London Calling North Pole*, p. 194. Lauwers, un agent SOE olandez capturat de germani, a încercat fără succes să informeze Londra cu privire la operaţiunea de dezinformare prin transmiterea unor mesaje fără a-şi lua însă măsurile de siguranţă necesare. Din nefericire, comandamentul a ignorat acest aspect şi a considerat mesajele autentice. Leo Marks, ofiţerul responsabil cu codurile SOE, sugerează că suspiciunile privind agenţii din Olanda au fost atenuate de temerea conducerii SOE că, dacă se

confirma un eşec de o asemenea anvergură, organizaţia ar fi fost închisă sau subordonată rivalului său din punct de vedere birocratic, Serviciului de informaţii externe, MI6. *Between Silk and Cyanid, The Story of the S.O.E.'s Code War* (HarperCollins, Londra, 199 o, pp. 112 – 125, 146 – 148.

58. Stansfield Turner, *Secrecy and Democracy*: *The CIA in Transition* (Houghton Mifflin, Boston, 1985; Harper and Row, 1986), p. 65.

59. Ca şi în alte cazuri, aici este necesar să se ajungă la un compromis. O variaţie pe orbită înseamnă că anumiţi sateliţi urmează orbite care nu au acoperire optimă; este necesar un echilibru între măsurile obişnuite de eficientizare a costurilor şi măsura mai subtilă de contracarare a operaţiunilor de acoperire şi de dezinformare ale adversarului.

60. David Kahn, expert în criptare, susţine acest punct de vedere în „Discussion" în Roy Godson (ed.), *Intelligence Requirements for the 1980's*: *Clandestine Collection* (National Strategy Information Center, Washington, DC, 1982), p. 119.

61. Andrew şi Gordievsky, *KGB*: *The Inside Story*, pp. 529 – 530, 610.

62. Procesele-verbale ale şedinţelor de planificare sunt reproduse în David E. Murphy, Serghei A. Kondrashev şi George Bailey, *Battleground Berlin*: *CIA vs. KGB in the Cold War* (Yale University Press, New Haven, Conn., 1997), pp. 449 – 453.

63. CIA a observat că un echipament electric de cifrare transmitea un semnal electric reprezentând un caracter obişnuit împreună cu caracterul cifrat; semnalul iniţial, deşi slab în comparaţie cu cel cifrat, putea fi receptat pe firul de transmisie, la o distanţă apreciabilă de echipamentul de cifrare. S-a descoperit că echipamentele sovietice de cifrare prezentau acelaşi dezavantaj, ceea ce le-a permis americanilor să recupereze atât mesajele cu caractere obişnuite, cât şi versiunile lor criptate. John Ranelagh. *The Agency*: *The rise and Decline of the CIA* (Simon and Schuster, New York, 1986), p. 140. Murphy şi colaboratorii săi, *Battleground Berlin*, neagă existenţa acestui „efect de ecou" (pp. 206 – 207). Este imposibil să lămurim acest aspect în lucrarea de faţă; relatarea din text are menirea de a ilustra tipul de implicaţii la care poate da naştere acest gen de operaţiuni.

64. Murphy *et* al, *Battleground Berlin*, p. 289.

65. Murphy *et* al, *Battleground Berlin*, p. 295.

66. De ce ar fi dorit sovieticii să încheie operaţiunea dacă avea drept scop transmiterea unor informaţii false? Ar fi putut face acest lucru pentru a dăuna moralului angajaţilor CIA ŞI MI6, considerând că puterile occidentale aveau să descopere oricum cât de curând adevărul despre această operaţiune. Sau sovieticii au pus capăt operaţiunii pur şi simplu deoarece costurile implicate de furnizarea „materialelor de dezinformare" (informaţii autentice oferite în mod voit inamicului pentru a întări credibilitatea operaţiunii) erau prea mari. Este posibil ca

descoperirea să fi fost făcută accidental, în sensul că echipa de intervenţie nu avea cunoştinţă de acest tunel, deoarece aceia care ştiau nu luaseră măsurile necesare pentru interzicerea lucrărilor în zona tunelului (dacă sovieticii desfăşurau o operaţiune de dezinformare numai un cerc restrâns de oameni avea cunoştinţă de acest lucru). Dacă SUA şi Marea Britanie ar fi aflat despre această descoperire, ar fi devenit suspicioase în momentul în care ruşii ar fi continuat să folosească în continuare cablul fără a îndepărta mijloacele de interceptare.

67. Cruickshank, *Deception in World War II*, 182.

68. Întreaga controversă a fost denumită „pustiul oglinzilor" şi este subiectul unei cărţi cu acelaşi titlu de David Martin (New York: Harper and Row, 1980).

Pentru mai multe lucrări recente pe marginea acestei controverse, vezi David Wise, *Molehunt: The Secret Search fot the Traitors that Shattered the CIA* (New York: Random House, 1992) şi lucrările citate în nota 35, capitolul 2.

69. John Barron, *Breaking the Ring* (Boston: Houghton Mifflin, 1987), 23-25.

70. Discuţia are ca sursă lucrările Comisiei senatoriale privind activitatea serviciilor de informaţii, *An Assessment of the Aldrich H. Ames Espionage Case*, 24-28.

71. În mod ironic, decizia KGB de a închide toate cazurile în acelaşi timp indică faptul că KGB *nu* a aflat despre acestea dintr-o singură sursă, foarte importantă; în caz contrar, nu ar fi acţionat

atât de ostentativ, deoarece acest lucru ar fi pus sursa în pericol. Potrivit lui Ames, cei de la KGB care se ocupau de el au recunoscut că decizia KGB il punea în pericol; i-au comunicat că „regretau faptul că l-au pus într-o asemenea situaţie, dar conducerea politică nu a avut de ales”. Comisia senatorială privind activitatea serviciilor de informaţii, *An Assessment*, 25.

72. Comisia senatorială privind activitatea serviciilor de informaţii, *An Assessment*, 46-53. Clayton Lonetree, un puşcaş marin care asigura paza ambasadei SUA din Moscova a avut o relaţie cu o rusoaică care lucra la KGB. Un coleg a declarat iniţial (dezminţind ulterior) că Lonetree i-a permis KGB-ului să pătrundă în clădirea ambasadei americane. Acest incident a produs confuzie în cadrul anchetei şi a distras atenţia de la posibilitatea – pe care CIA se temea oricum să o ia în considerare – ca sursa problemelor să fi fost un ofiţer CIA.

73. Comisia senatorială privind activitatea serviciilor de informaţii, *An Assessment*, 64-66. Din diferite motive, acest pont primit în noiembrie 1989, nu a fost exploatat suficient; Ames a fost arestat abia în luna februarie 1994.

## Capitolul 6. Controlul paznicilor: managementul culegerii informaţiilor

1. Deşi senatorul Church, preşedintele Comisiei senatoriale înfiinţate lui 1975 pentru investigarea activităţii serviciilor de informaţii, a foloall sintagma *oaie rătăcită* la începutul

investigaţiei pentru a desemna CIA; această caracterizare a fost abandonată până la încheierea investigaţiei. Conform lui Loch Johnson, un membru al comisiei Church care îl susţinea pe senator, explica faptul că preşedintele comisiei folosise această expresie deoarece „avea sentimentul că impactul probelor trebuia exagerat pentru a avea efect asupra publicului”, în timp ce raportul final al comisiei „evita cu grijă teoria «oii rătăcite»”. Loch Johnson, *A Season of Inquiry*: *The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, Lexington, 1985), pp. 224, 268.

2. US Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Alleged Assassination Plots Involving Foreign Leaders*: *Interim Report*, Congresul al 94-lea, prima şedinţă, 1975, S. Rept 94 – 94, 263.C

3. Pe 7 mai 1962, procurorul general Robert F. Kennedy a fost informat oficial cu privire la acţiunile întreprinse în 1960 – 1961 în vederea asasinării lui Castro, subliniindu-se implicarea CIA în acest sens alături de doi membri ai Mafiei, John Roselli şi Sam Giancana. Necesitatea unei anchete oficiale a survenit din cauza faptului că FBI intenţiona să îl pună sub acuzare pe Robert Maheu, omul de legătură dintre CIA şi Mafie, pentru instalarea unor dispozitive de interceptare ilegale, iar CIA dorea să împiedice această măsură, pentru ca întreaga poveste să nu fie dezvăluită. Se spune că Kennedy s-ar fi înfuriat aflând de implicarea Mafiei, ceea ce ar fi

complicat punerea sub acuzare a lui Roselli sau Giancana pentru posibile acţiuni de tip crimă organizată; se pare că nu ar fi fost la fel de furios când a aflat de încercarea de asasinat. Select Committee, *Alleged Assassination Plots*, pp. 131 – 134.

4. Cea mai bună dovadă în acest sens o reprezintă faptul că membrii administraţiei nu s-au arătat deloc indignaţi atunci când operaţiunile împotriva lui Castro au devenit publice. În mod evident, aceasta este o atitudine de genul „nici usturoi nu a mâncat...”; cu toate acestea, era de aşteptat ca membri importanţi ai administraţiei Kennedy, cum ar fi fostul secretar de stat al Apărării Robert McNamara, să se arate iritaţi de faptul că CIA s-a implicat în astfel de activităţi fără să primească aprobare de mai sus. În schimb, McNamara a subliniat, în faţa Comisiei Church, că, după părerea sa, „CIA era o organizaţie extrem de disciplinată, perfect controlată de importanţi membri ai guvernului” (Select Committee, *Alleged Assassination Plots*, p. 159, citând depoziţia lui McNamara din 11 iulie 1975). Se pare că reacţia lui Robert Kennedy din 1962 a fost similară; vezi nota anterioară.

5. Christopher Andrew, *Her Majesty’s Secret Service*: *The Making of the British Intelligence Community* (Viking, New York, 1986), p. 1.

6. Winston S. Churchill, *Marlborough*: *His Life and Times* (Scribner, New York, 1938), vol. 6, pp. 482 – 484, 526 – 529. Oponenţii lui Marlborough susţineau că aceşti bani reprezentau fonduri publice şi trebuia să se dea socoteală

pentru ei; datorită faptului că a folosit fondurile pentru a-şi plăti agentura, acest lucru ar fi fost imposibil. Churchill susţine cu tărie că ilustrul său strămoş a procedat corect folosind sursele tradiţionale de bani pentru a finanţa activităţile de culegere a informaţiilor, care nu erau finanţate de guvern.

7. La începuturile republicii americane s-a încercat aproximarea vechiului sistem, Congresul stabilind un fond pentru situaţii neprevăzute aflat la discreţia preşedintelui care să poată fi folosit pentru a plăti persoanele ce „servesc SUA în afara teritoriului ţării. Preşedintele era obligat să informeze Congresul numai despre faptul că banii au fost cheltuiţi; nu trebuiau divulgate nici scopul plăţilor şi nici numele celor care primeau aceste plăţi. Primii preşedinţi recurgeau la persoane private care desfăşurau anumite acţiuni peste hotare; aceşti „agenţi" erau numiţi fără aprobarea Senatului. În privinţa înfiinţării fondului şi despre modul în care erau utilizaţi aceşti agenţi, vezi Stephen F. Knott, *Secret and Sanctioned*: *Covert Operations and the American Presidency* (Oxford University Press, New York, 1996), pp. 49 – 60.

8. Prevederile au apărut iniţial în deciziile prin care se hotăra înfiinţarea comisiilor privind activitatea serviciilor de informaţii din Senat şi din Camera Reprezentanţilor şi au fost formulate sub forma unei legi în 1980; cu schimbări minore, acestea au devenit Legea autorizării informaţiilor secrete din 1991. Prevederile de interes sunt reprezentate de secţiunile 501 şi 502 din Legea privind securitatea naţională din 1947.

9. Robert M. Gates, „The CIA and American Foreign Policy”, *Foreign Affairs*, 66, nr. 2 (iarna 1987 – 1888), p. 225. Potrivit acesteia, „Congresul a primit peste 1.000 informări ale CIA şi 7.000 rapoarte de informaţii în 1991”. Loch K. Johnson, „Smart Intelligence”, *Foreign Policy*, nr. 89 (iarna 1992 – 1993), p. 67. În anii ’90 tendinţa a continuat: Legea autorizării informaţiilor secrete din 1990 (PL 101-193, 30 noiembrie 1989) a stabilit ca numirea inspectorului general (IG) al CIA să fie confirmată de Senat. În plus, legea prevedea ca directorul CIA să înainteze comisiilor de supraveghere copii ale rapoartelor bianuale ale IG. Aşadar, în 1999, prin Legea autorizării informaţiilor secrete (PL105 – 272, 20 octombrie 1998), Congresul a adoptat o serie de prevederi menite să îi protejeze pe aşa-numiţii „informatori” din comunitatea de informaţii, Legea prevede o serie de proceduri prin care angajaţii serviciilor secrete pot furniza informaţii în situaţii speciale comisiilor de supraveghere prin inspectorul general al serviciului şi prin director. Vorbind despre această măsură, preşedintele comisiei din Camera Reprezentanţilor a precizat: „Am deschis o uşă pentru a înlesni schimbul de informaţii cu Congresul”. *Congressional Record*, 7 octombrie 1997, H9729.

10. Realitatea acestui „domeniu privat” a fost întărită de teoriile din domeniul administraţiei publice, care subliniau distincţia dintre „realitate şi valoare”, încercau să facă o distincţie între cei ce elaborau politicile şi componenta birocratică (administraţia) a căror datorie era implementarea

unei politici în modul cel mai eficient şi mai raţional. Pentru varianta americană tradiţională a acestei teorii, vezi Woodrow Wilson, „The Study of Administration”, *Pölitical Science Quarterly*, *2* (iunie 1887), pp. 197 – 222. Puţini specialişti din acest domeniu mai iau în considerare această diferenţă în ziua de azi, dar rămâne în continuare (în absenţa unui punct de vedere alternativ coerent) principala teorie printre cei din administraţie, dar şi printre cei ce urmăresc reformarea administraţiei.

11. Într-o mai mică măsură, această teorie de organizare este reflectată de decizia Marii Britanii din 1983 ca preşedintele Comisiei mixte pentru activitatea de informaţii (Joint Intelligence Committee – JIC, agenţia guvernamentală britanică responsabilă cu coordonarea activităţii de culegere de informaţii şi a evaluărilor la nivel naţional) să fie numit de prim-ministru din rândul echipei guvernamentale; anterior, preşedintele fusese ales din rândul angajaţilor Ministerului de Externe. Schimbarea recomandată de o comisie de anchetă (Comisia Franks) însărcinată cu evaluarea activităţii serviciilor secrete britanice în timpul crizei Falklands avea drept scop să îi confere preşedintelui JIC un „rol mai important şi mai multă independenţă”. Pentru mai multe detalii privind ancheta Comisiei Franks, vezi Robert Cecil, „The Assessment and Acceptance of Intelligence: A Case-Study”, în K.G. Robertson (ed.), *British and American Approaches to Intelligence* (Macmillan, RUŞI Defense Studies Séries, Londra, 1987), pp. 166 – 183. În mod

similar, avântul iniţial pentru crearea Agenţia de informaţii a armatei americane (Defense Intelligence Agency – DIA) putea fi atribuit, cel puţin parţial, dorinţei de a înfiinţa (în cadrul Departamentului de Apărare) o agenţie centralizată de evaluare care să fie independentă de vederile înguste şi interesele serviciilor militare şi ale agenţiilor lor de informaţii. Pentru mai multe detalii privind efortul mai mult decât neizbutit de a înfiinţa DIA conform acestor principii, vezi Patrick Mescall, „The birth of the defense Intelligence Agency", în Rhodri Jeffreys-Jones şi

Andrew Lownie (ed.), *North American Spies*: *New Revisionist Essays* (University Press of Kansas, Lawrence, 1991), pp. 158.201

12. Graham E. Fuller, „Intelligence, Immaculately Conceived", *The National Interest*, nr. 26 (iarna 1991 – 1992), p. 98.

13. *Antony and Cleopatra*, 2.5.85 – 88.

14. Cel mai renumit teoretician militar, Carl von Clausewitz, care se arăta foarte sceptic în privinţa acurateţii şi a valorii majorităţii rapoartelor de informaţii, considera că un comandant trebuia să dea dovadă de capacitatea de a defini clar obiectivele activităţii desfăşurate: „Comandantul trebuie să aibă încredere în judecata sa şi să fie ca o stâncă într-o mare [de informaţii false]". Carl von Clausewitz, *On War*, ediţie îngrijită şi traducere de Michael Howard şi Peter Paret (Princeton University Press, Princeton NJ, 1976), p. 117.

15. Henry Brandon, *The Retreat of American Power* (Doubleday, New York, 1973), p. 103. Se

spune că preşedintele Johnsons a făcut această remarcă la o cină la Casa Albă în compania directorului Richard Helms.

16. „Managing/Teaching New Analysts”, *Studie* se în *Intelligence*, 30, nr. 3 (toamna 1986), pp. 3 – 4. Numele autorului (se pare un director din cadrul Directoratului pentru informaţii secrete, CIA) a fost şters ca răspuns la o cerere înaintată pe baza Legea privind accesul liber la informaţii. Îi sunt recunoscător lui Eliot Cohen pentru că mi-a atras atenţia în privinţa acestui articol. Acesta discută articolul în „Analysis”, în Roy Godson (ed.), *Intelligence Requirements for the 1990's*: *Collection*, *Analysis*, *Counterintelligence and Covert Action* (Heath, Lexington, Lexington, Mass., 1989), pp. 71 – 96.

17. Cohen, „Analysis”, p. 76.

18. Charles H. Fairbanks Jr., „Where is the Secret?”, *The Washington Post*, *25* februarie 1987, p. A23 [subliniere în original].

19. Fairbanks, „Where Is the Secret?”

20. Fuller, „Intelligence Immaculately Conceived”, pp. 96 – 97. Cu toate acestea, pentru Fuller caracterul ideologic inerent al analizei informaţiilor secrete strategice nu pare să aibă niciun fel de implicaţii în ceea ce priveşte relaţia dintre informaţiile secrete şi cele strategice. Îndeosebi, acesta nu pare să fie de acord cu opinia factorilor de decizie conform căreia strategia bazată pe informaţii secrete poate submina strategia administraţiei (vezi *supra*, nota 12). Din punctul de vedere al unui analist de informaţii secrete, Fuller pledează pentru independenţă

(posibilitatea de a putea ignora poziţia factorilor de decizie), dar nu abordează argumentele care ar putea justifica acest lucru.

21. Bob Woodward şi Dan Morgan, „Soviet Threat toward Iran Overstated, Casey Concluded”, *The Washington Post*, 13 ianuarie 1987, p. Al.

22. Loch K. Johnson, *Secret Agencies*: *US Intelligence* în *a Hostile World* (Yale University Press, New Haven, Conn., 1996), p. 129.

23. Robert M. Gates, „The CIA and Foreign Policy”, *Foreign Affairs*, 66, nr. 2 (iarna 1987 – 1988), p. 221.

24. Această secţiune se bazează pe lucrarea lui Abram N. Shulsky şi Gary Schmitt, *The Future of Intelligence*: *Report Prepared for the Working Group on Intelligence Reform* (Consortium for the Study of Intelligence, DC, Washington, 1996), pp. 14 – 16.

25. Legea securităţii naţionale din 1947, secţiunea 501(a) (1), conform amendamentelor [50 USC 413].

26. Gates, „The CIA and Foreign Policy”, pp. 225.

27. Legea privind controlul activităţii de informaţii din 1980 menţiona clar că „prevederea anterioară nu va necesita aprobarea din partea comisiilor pentru controlul activităţii de informaţii anterior iniţierii unei astfel de activităţi de informaţii [operaţiune secretă]”. Legea autorizării informaţiilor secrete din 1991, ce revedea cerinţele privind raportarea operaţiunilor secrete în faţa Congresului, prevedea o solicitare similară. Legea securităţii naţionale din 1947, conform

amendamentelor, sect. 501(a) (1) [50 USC 413(a) (3)]. O astfel de ocazie când comisiile şi-au exercitat dreptul de veto a apărut legat de o propunere a administraţiei Bush din 1989 de a asigura ajutor secret forţelor potrivnice lui Noriega în Panamá. Vezi Stephen Engleberg, „US Officials Say Senators Balked At Noriega Ouster", *The New York Times*, 24 aprilie 1989, p. Al.

28. Un alt exemplu al folosirii făţişe a puterii financiare în detrimentul operaţiunilor secrete îl reprezintă asistenţa acordată rezistenţei anticomuniste din Cambodgia. În *Conference Report* ce însoţea Legea autorizării informaţiilor secrete din 1991 înaintat în octombrie 1990, cele două comisii pentru controlul activităţii de informaţii au precizat pe larg tipul de asistenţă ce urma să fie acordată (neletală) şi în ce scop (promovarea unui acord de pace). US House of Representatives, Permanent Select Committee on Intelligence, *Conference Report*: *Intelligence Authorization Act for Fiscal Year 1991*, Congresul al 101-lea, şedinţa a doua, H. Rept. 101 – 928, 34. Congresul a blocat cererea administraţiei Bush de alocarea unor fonduri pentru ajutor militar letal către forţele anticomuniste din Cambodgia. Peter Rodman, „Supping with Devils", *The National Interest*, nr. 25 (toamna 1991), p. 47.

29. Datele despre scurgerile de informaţii sunt nu numai rare, ci pot, totodată, să inducă în eroare. Referirea într-un articol la o „sursă din Congres" sau la „un funcţionar din administraţie" nu va indica neapărat sursa jurnalistului; sursa originală a făcut practic imposibilă orice referire

la ea. Astfel referirea din articol poate trimite către o sursă care a comentat pe marginea unor aspecte dintr-o informaţie deja deţinută de jurnalist, şi nu la sursa originală. Leon V. Sigal, *Reporters and Officials*: *The Organization and Politics of Newsmaking* (Heath, Lexington, Mass., 1973) discută pe marginea acestor tactici care îi permit unui funcţionar „să îşi asigure un alibi”.

30. Comisia senatorială privind operaţiunile guvernamentale referitoare la activităţile de culegere a informaţiilor, *Final Report*, vol. I: *Foreign and Military Intelligence*, Congresul al 94-lea, şedinţa a doua, 1976, S. Rept. 94.755, 522. Halperin susţinea abolirea dreptului de a desfăşura operaţiuni secrete.

31. După cum a remarcat Samuel Huntington: „Într-o atmosferă diferită… comisiile din Congres care investigau activitatea CIA ar fi putut arăta curiozitate în privinţa eşecului Agenţiei de a-i asasina pe Lumumba şi Castro… [cu toate acestea, la momentul respectiv], nimeni nu era interesat dacă Agenţia avea capacitatea de a îndeplini ordinele primite, singurul lucru care suscita interes era caracterul lor imoral”. Huntington, *American Politics*: *The Promise of Disharmony* (Harvard University Press, Cambridge, Mass., 1981), p. 191.

32. Pentru o prezentare a sistemului canadian, vezi Geoffrey R. Weiler, „Accountability în Canadian Intelligence Services”. *International Journal of Intelligence and Counterintelligence*, *2*, nr. 3 (toamna 1988), pp. 415 – 441, şi Reg Whitaker, „The Politics of Security Intelligence

Policy – making în Canada: II, 1984", *Intelligence and National Security*, 7, nr. 2 (aprilie 1992), pp. 53 – 76.

33. Vezi Frank Cain, „Accountability and the Australian Security Intelligence Organization: A Brief History", în A. Stuart Farson, David Stafford şi Wesley K. Wark (eds.), *Security and Intelligence in a Changing World*: *New Perspectives for the 1990's*, (Frank Cass, Londra, 1991), pp. 10 – 24, 104 – 125.

34. În general, foarte puţine informaţii au fost făcute publice privind supravegherea activităţii de informaţii în alte ţări decât cele deja menţionate. Deşi au apărut noi reglementări privind activitatea de supraveghere în mai multe ţări, s-au publicat destul de puţine lucrări care descriu şi compară diverse sisteme de supraveghere. Alfred B. Prados şi Richard A. Best, „Intelligence Oversight in Selected Democracies", CRS Rept. 90.483, Congressional Research Service, Library of Congress, 21 septembrie 1990, deşi o publicaţie mai veche, aceasta rămâne o sursă valoroasă pe acest subiect.

35. Legea privind activitatea serviciilor secrete 1994, sect. 10 (3), *apud* House of Commons, Select Committee on Home Affairs, *Third Report*: *Accountability of the Security Service*, 14 iunie 1999. Raportul este disponibil şi pe www. fas.org/irp/world/uk/docs/291/29102.htm.

36. House of Commons, *Third Report*. Sistemul de supraveghere din Nour Zeelandă îi conferă prim-ministrului puteri sporite. În 1996, în urma Legii de înfiinţare a comisiei pentru

siguranţă şi controlul activităţii de informaţii, a luat naştere comisia de supraveghere a activităţii de informaţii cu următoarea componenţă: prim-ministrul, liderul opoziţiei, doi membri ai parlamentului aleşi de premier şi un membru al opoziţiei ales de liderul acesteia. Deşi mandatul extins al comisiei prevede „examinarea strategiei, a modului de administrare şi a cheltuielilor fiecărui serviciu de informaţii şi securitate”, autoritatea sa de supraveghere este limitată de faptul că premierul şi cei numiţi de acesta deţin majoritatea în comisie, iar premierul este singurul care poate solicita audieri. În plus, comisia nu are dreptul să investigheze „nicio problemă sensibilă din punct de vedere operativ, inclusiv orice problemă legată de culegerea de informaţii şi metodele producere şi sursele informaţiilor”. Legea poate fi găsită pe rangi. knowledge-basket.co. nz./gpacts/public/text/1996/se/046 sel.html.

37. Site-ul parlamentului australian: www.aph. gov. au/house/committee/plcasio/ppgrole.htm.

38. „Dreptul oamenilor de a fi protejaţi... împotriva unor anchete şi confiscări de bunuri nemotivate nu va fi încălcat şi nu vor fi emise mandate, decât în cazuri justificate. „Constituţia Statelor Unite, al Patrulea Amendament.

39. PL. 95 – 5U [50USC 1801 – 11]. Pentru o prezentare a legii şi a elaborării acesteia, vezi Americo R. Cinquegrana, „The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978”,

*University of Pennsylvania Law Review*, 137 (ianuarie 1989), pp. 793 – 828, şi Elizabeth B. Bazan, „The Forcing Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance", Congressional Research Service, Library of Congress, 17 mai 2000.

40. Legea autorizării informaţiilor secrete din 1995 (PL 103 – 359, 14 octombrie 1994), sec. 807. „Ancheta fizică" este definită drept „orice pătrundere... în spaţii sau pe o proprietate... ce are drept scop confiscarea... sau alterarea unor informaţii, materiale ori bunuri, în condiţiile în care persoana respectivă are dreptul la o viaţă privată, un mandat fiind necesar în scopul punerii în aplicare a legii, dar nu include [informaţii obţinute din transmisii radioelectronice]".

41. Într-un studiu detaliat numit „The Study of Intelligence in the United States", Kenneth G. Robertson remarcă: „Până în prezent s-a cercetat destul de puţin natura ameninţărilor interne şi modul în care acestea pot influenţa cerinţele privind informaţiile secrete obţinute de pe teritoriul ţării". În Roy Godson (ed.), *Comparing Foreign Intelligence*: *The US*, *the USSR*, *the UK and the Third World* (Pergamon-Brassey's, McLean. Vancouver, 1988), p. 19. Situaţia nu s-a schimbat semnificativ de la publicarea studiului lui Robertson.

42. Desigur, nu toate infracţiunile sunt importante din punctul de vedere al informaţiilor secrete obţinute de pe teritoriul ţării; standardul infracţional nu stabileşte ceea ce ar fi de interes pentru activitatea de culegere a informaţiilor de

pe teritoriul ţării, ci mai degrabă ceea ce nu face obiectul acestei activităţi. În general, culegerea unor informaţii legate de punerea în aplicare a legii vizează mai degrabă crima organizata – Mafia şi activităţile gangsterilor, traficul de droguri pe scara largă decât actele infracţionale sporadice.

43. Potrivit acestei legi, supravegherea electronică a „persoanelor cu cetăţenie americană” (cetăţeni sau persoane de origine străină cu drept de reşedinţă permanent) este permisă doar dacă există „motive întemeiate” pentru a le suspecta de implicare cu bună ştiinţă în acte de sabotaj în favoare unei puteri străine, terorism internaţional sau alte activităţi clandestine de culegere a informaţiilor care presupun încălcarea legilor penale.

44. O variantă adaptată a acestor principii a fost elaborată în urma unei cereri pe baza Legea privind libertatea informaţiilor şi a apărut în US Senate, Select Committee on Intelligence, *National Intelligence Reorganization and Reform Act of 1978*: *Hearings*, Congresul al 95-lea, şedinţa a doua, Committee Print, pp. 774 – 790.

45. US Senate, Select Committee on Intelligence, *Hearings*, paragraful ILA, p. 775 [subliniere în original].

46. Legea înregistrării agenţilor străini din 1938 prevede: deconspirarea numelor persoanelor implicate în activităţi de propagandă sau alte tipuri de activităţi pentru sau în numele unor ţări străine astfel încât guvernul şi cetăţenii Statelor Unite să poată fi informaţi cu privire la identitatea acestor persoane, putându-le evalua afirmaţiile şi

acţiunile în strânsă legătură cu mediile frecventate şi activităţile derulate. Citatul este extras din legea mai sus menţionată, secţiunea privind „Politica şi obiectivele”. Legea în sine, exceptând această afirmaţie, este criptată la 22 USC 611 – 21.

47. Pe 9 februarie 1989, Alan Thomson, directorul Naţional Council of American-Soviet Friendship, a fost arestat după constituirea unui depozit bancar de 17.000 de dolari în bani lichizi. Se pare că suma ar fi fost furnizată de Asociaţia Sovietică pentru Prietenie şi Relaţii Culturale cu alte state, care, potrivit unui raport FBI, se afla sub controlul Departamentului Internaţional al Comitetului Central al Partidului Comunist din Uniunea Sovietică. Aceasta fiind prima decizie de punere sub arest din Statele Unite, corelată cu măsuri eficiente sau misiuni secrete ale Uniunii Sovietice, acuzaţia propriu-zisă s-a bazat mai curând pe nedeclararea acestor transferuri importante de bani (conform prevederilor referitoare la combaterea activităţilor de spălare a banilor) decât pe neînregistrarea persoanei în cauză drept cetăţean străin. (Associated Press, 8 februarie 1989; *The Washington Post*, 8 februarie 1989, p. A4.) în mai 1992, Thomson a recunoscut că se face vinovat de nedeclararea banilor la intrarea în Statele Unite, după cum stipulează reglementările vamale în vigoare. Dan Herbeck, „Man Fined 1, 1.000 Dollars for Not Declaring Cash”, *Buffalo News*, 31 iulie 1992 (secţiunea cu ştiri locale).

48. US Senate, Select Committee on

Intelligence, *The FBI and CISPES*: *Report*, Congresul al 101-lea, prima şedinţă, S. Rept, pp. 101 – 146, 21. O anchetă amănunţită a CISPES a fost iniţiată ulterior de FBI pe temeiuri complet diferite.

49. În 1983, Levi Domestic Security Guidelines a fost înlocuit cu „Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/ Terrorism Investigations", aprobat de procurorul general William French Smith. Vezi Roy Godson, *Intelligence Requirements for the 1980's*: *Domestic Intelligence* (Heath, Lexington, Mass., 1986), pp. 225 – 264. Pentru o privire de ansamblu asupra lucrării lui Smith şi a compatibilităţii cu lucrarea lui Levi, vezi John T. Elliff, „The Attorney General's Guidelines for FBI Investigations", *Cornell Law Review*, 69, nr. 4 (aprilie 1984), 785 – 815.

50. Levi, „Domestic Security Guidelines", paragraful I.A., în Godson (ed.), *Domestic Intelligence*, p. 225.

51. Lucrarea lui Levi nu face o referire clară la acest aspect; în schimb, în lucrare se precizează că „toate anchetele derulate în conformitate cu reglementările conţinute în această lucrare vor fi iniţiate şi conduse astfel încât să nu impieteze exercitarea deplină a drepturilor prevăzute prin Constituţia şi legislaţia Statelor Unite" (paragraful II B). Astfel, nu se ştie exact dacă ancheta propriu-zisă limitează dreptul la liberă exprimare prin descurajarea acesteia; de aceea, o anchetă bazată numai pe ideea protejării dreptului la exprimare al unui individ sau al unei grupări ar încălca această

prevedere. În acest context, unul dintre cele mai controversate aspecte legate de lucrarea lui Smith l-a constituit prevederea potrivit căreia FBI poate demara o anchetă numai în baza unor afirmaţii care „sprijină infracţionalitatea sau care indică o intenţie aparentă de a comite o infracţiune”. În schimb, lucrarea lui Levi nu face nicio referire la anchetele bazate numai pe acest gen de afirmaţii. Cu toate acestea, după cum s-a putut vedea şi din citatul de mai sus, afirmaţiile ce ar putea prezenta interes în derularea anchetei sunt stabilite în funcţie de standardele de infracţionalitate prevăzute în lucrarea lui Smith.

52. *Laird* v. *Tatum*, 408 US l-10 (1972), 13 – 14.

53. Robertson, „The Study of Intelligence in the United States”, pp. 18 – 21.

54. *Brandenburg* v. *Ohio*, 395 US 444 – 447 (1969) [sublinierea noastră].

55. *Scales v. United States*, 367 US 203 – 220 (1961). Curtea Supremă parafrazează şi (în cazul afirmaţiilor plasate între ghilimele) citează recomandările judecătorului în faţa juriului; ulterior, Curtea Supremă aprobă aceste recomandări (224).

56. John T. Elliff, *The Reform of FBI Intelligence Operations* (Princeton University Press, Princeton, NJ, 1979), p. 57.

57. Desigur, gruparea ar trebui să aibă o capacitate de autocontrol extraordinară pentru a nu comite acte de violenţă sau alte acte prin care se încalcă legea, în perioada în care încearcă să se infiltreze în guvern. Se pare că grupările de

extremă dreapta care activează în prezent în Statele Unite şi în alte state democratice nu sunt atât de experimentate.

58. Shlomo Gazit şi Michael Handel, „Insurgency, Terrorism and Intelligence", în Godson (ed.), *Domestic Intelligence*, p. 134.

59. Standardele stabilite („limitările") diferă de la o lucrare la alta. Potrivit lui Levi, FBI nu poate folosi un informator decât dacă are „dovezi palpabile care să demonstreze faptul că... o grupare este sau ar putea fi implicată în activităţi ce presupun recurgerea la forţă sau violenţă şi care implică sau ar putea implica încălcarea legii federale" (secţiunea II [I], 227 – 228. Potrivit lui Smith, într-o anchetă „preliminară" poate fi folosit un informator cu aprobarea agentului numai în caz de necesitate sau dacă alte metode de investigaţie mai puţin invazive nu sunt eficiente. O „anchetă preliminară" poate fi demarată în cazul în care FBI primeşte informaţii privind o posibilă infracţiune ce, chiar dacă „nu impune o anchetă detaliată", presupune o serie de eforturi în scopul verificării pistelor iniţiale (secţiunea II [B][1][6], 248 – 251).

60. Acest citat, precum şi următoarele două, sunt preluate din John M. Walker Jr., „Discussion", în Godson (ed.), *Domestic Intelligence*, pp. 194 – 196.

61. Atorney General (Smith) Guidelines on Domestic Security, III. B.1(a), în Godson (ed.), *Domestic Intelligence*, p. 258.

62. David M. Park, „Re-examining the Attorney Generalis Guidelines for FBI

Investigations of Domestic Groups", *Arizona Law Review* (vara 1997), p. 774, citează mărturia lui Freeh în faţa US House of Representatives, International Relations Committeee, Crime Subcommittee, *Terrorism Hearings*, Congresul al 104-lea, prima şedinţă, 1995, p. 12.

63. Smith Guidelines, III B.1(a), în *Domestic Intelligence*, Godson (ed.), p. 258.

64. Mărturia lui Laurence H. Silberman, 18 iulie 1978, în US Senate, Select Committee on Intelligence, *Hearings*, p. 616.

65. Church Committee, *Final Report*, vol. 2: *Intelligence Activities and the Rights of Americans*, Congresul al 94-lea, şedinţa a doua, 1976, S. Rept. 94 – 755, 166. Odată cu publicarea lucrării lui Levi, numărul anchetelor pe tema securităţii interne a scăzut semnificativ. În aprilie

1976, au fost demarate 4.868 de anchete; până la sfârşitul lui septembrie, au fost iniţiate numai 626. În august 1982, erau în curs de desfăşurare numai 38 de anchete privind securitatea internă. US Senate, Subcommittee on Security and Terrorrism, Committee on the Judiciary, *Impact of Attorney General's Guidelines for Domestic Security Investigations (The Levi Guidelines)*: *Hearing*, Congresul al 98-lea, prima şedinţă, 1983, S. Prt. 98 – 134, 5.

66. Church Committee, *Final Report*, vol. 2, 225 – 240, face referire la cazurile ce au furnizat informaţii strict politice, care au fost trimise factorilor de decizie din domeniul administrativ.

67. Legea privind activitatea serviciilor secrete canadiene, 1984, secţiunile 2 şi 12.

Potrivit legislaţiei canadiene, atribuţiile de culegere şi analiză a informaţiilor secrete privind ameninţările la adresa securităţii, precum şi cele de evaluare a personalului din sfera securităţii revin CSIS, în timp ce poliţia călare canadiană este responsabilă cu aplicarea legislaţiei referitoare la securitatea naţională şi garantarea protecţiei şi securităţii guvernanţilor şi a obiectivelor guvernamentale. Puteţi găsi această lege http://www.csis-scrs. gc. ca/end/act/csisact_e.html.[2]

**Capitolul 7. Două perspective asupra lumii informaţiilor**

1. Sun Tzu, *The Art of War* (Oxford University Press, Oxford, 1964), pp. 144 – 145 (capitolul 13, paragrafele 3 – 4). „Tzu" este varianta romanizată (transcrisă în alfabet latin) învechită, dar familiară a unui personaj chinezesc care s-ar traduce, în zilele noastre, prin „Zi".

2. Sun Tzu, *The Art of War*, p. 146 (capitolul 13, paragrafele 9 – 10).

3. Sun Tzu, *The Art of War*, pp. 77 – 78 (capitolul 3, paragrafele 4 – 6). Acest punct de vedere contrastează cu cel al lui Carl von Clausewitz, care consideră că anihilarea forţelor militare inamice este esenţială. Carl von Clausewitz, *On War*, ediţie îngrijită şi traducere de Michael Howard şi Peter Paret (Princeton University Press, Princeton, NJ, 1976), p. 90 (vol. 1, capitolul 2). După cum s-a putut remarca, Clausewitz se arată mult mai sceptic în privinţa

2 http://laws-lois.justice.gc.ca/eng/acts/C-23/

şansei ca informaţiile secrete să permită implicarea unui comandant în misiuni grele, care să se finalizeze cu o victorie şi să implice costuri minime. Acesta afirmă că, „pe scurt, majoritatea informaţiilor secrete sunt false” (p. 117, vol. 1, capitolul 7).

4. William E. Colby, „Intelligence in the 1980’s”, *The Information Society*, 1, nr. 1 (1981), pp. 53 – 54.

5. Colby, „Intelligence in the 1980’s”, p. 65.

6. Pe 11 iulie 1941, preşedintele Roosevelt a decretat înfiinţarea „Departamentului de Informaţii Secrete, cu atribuţii de culegere şi analiză a informaţiilor şi datelor ce ar putea aduce atingere securităţii naţionale, atribuţii de procesare a acestor informaţii şi date, precum şi de informare a preşedintelui, a ministerelor şi a oficialilor abilitaţi de preşedinte să le cunoască…” (decret prezidenţial, „Designating a Coordinator of Information”, paragraful 1). Decretul a fost republicat în Thomas F. Troy, *Donovan and the CIA*: *A History of the Establishment of the Central Intelligence Agency* (University Publications of America, Frederick, Md., 1981), p. 423.

7. Colby, „Intelligence in the 1980’s”, p. 54.

8. Pentru o polemică privind incapacitatea de procesare şi de analiză a Departamentului OSS, care se ocupă de partea analitică a operaţiunilor CIA, vezi Ray S. Cline, *The CIA*: *Reality vs. Myth*, ediţie revizuită (Acropolis, Washington, DC, 1982), pp. 78, 80 – 81. Cline precizează că „[nicio] componentă a OSS nu a folosit vreodată în rapoartele sale informaţii obţinute din transmisii

radioelectronice” (p. 78). De aceea, nu a avut acces la majoritatea surselor de informaţii secrete (Ultra şi Magic) aflate la dispoziţia guvernului Statelor Unite.

9. Sherman Kent, *Strategic Intelligence for* American *World Policy* (Princeton University Press, Princeton, NJ, 1949; republicată cu o nouă prefaţă, 1966), p. 155. Recomandările lui Kent referitoare la serviciile de informaţii au fost acceptate din două motive. Aşa cum Berkowitz şi Goodman au subliniat, „*Strategic Intelligence* a fost probabil cea mai inspirată carte despre analiza informaţiilor secrete scrisă vreodată. A devenit o lucrare de referinţă nu numai pentru studenţii americani care doreau să devină ofiţeri de informaţii, ci şi în afara graniţelor, fiind ulterior tradusă în franceză, rusă, germană şi în alte limbi”. În plus, după eşecul comunităţii serviciilor de informaţii, care nu a reuşit să împiedice, în 1950, invadarea Coreei de Sud de către Coreea de Nord, Walter Smith (zis „Beedle”), directorul agenţiei, a solicitat înfiinţarea „unui nou departament care să se ocupe de evaluarea dinamică şi minuţioasă a informaţiilor secrete. Aceste rapoarte au devenit cunoscute sub numele Evaluări Informative Naţionale (NIE), iar instituţia s-a numit Biroul pentru Evaluări Informative Naţionale (ONE)”. Kent a fost desemnat primul director adjunct al ONE, iar în 1952 a devenit directorul Biroului, poziţie pe care şi-a păstrat-o timp de 16 ani. „Nu este nevoie să mai menţionăm”, au precizat Berkowitz şi Goodman, „că ONE şi modul de realizare a rapoartelor se

aseamănă, într-o mare măsură, principiilor analitice descrise de Kent în *Strategic Intelligence*". Bruce D. Berkowitz şi Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton University Press, Princeton, NJ, 1989), pp. 4 – 5.

10. Kent, *Strategic Intelligence*, pp. 3 – 4 [sublinierea autorului].

11. Colby, „Intelligence in the 1980's", p. 59. „Clubul de la Roma" a publicat, la sfârşitul anilor '70, o serie de studii despre tendinţele demografice, economice şi conjuncturale proiectate pentru secolul XXI. Previziunile sale s-au dovedit extrem de pesimiste.

12. Potrivit lui Alexander Orlov, un defector din NKVD, în contextul creat de Uniunea Sovietică, analiza sau evaluarea „ţine mai degrabă de stabilirea autenticităţii documentelor furate decât de importanţa informaţiilor. Importanţa politică a informaţiilor este evaluată mai întâi de factorii de decizie politici din cadrul guvernului şi ai prezidiului executiv [Politbüro] Alexander Orlov, *Handbook of Intelligence and Guerilla Warfare* (University of Michigan Press, Ann Arbor, 1965), p. 187. O polemică interesantă cu privire la importanţa analizei a pornit de la sistemul de radiolocaţie (DISTANT) pe care MI6 (serviciul de informaţii britanic) şi CIA i l-au pus la dispoziţie lui Oleg Penkovsky pentru a-l folosi în cazul în care ar fi intrat în posesia unor informaţii privind un atac iminent al Occidentului asupra Uniunii Sovietice. Potrivit unui studiu detaliat despre cazul Penkovsky, MI6 „se temea că un semnal de

avertizare transmis prin intermediul sistemului de radiolocaţie DISTANT poate să fie interpretat greşit sau să conducă la ostilităţi, dacă nu este evaluat şi supravegheat cu atenţie”. Marea Britanie era convinsă că orice avertizare ar trebui să fie mai întâi procesată de Comisia Mixtă pentru Activitatea de Informaţii (JIC), forul britanic superior de evaluare a informaţiilor, înainte de a ajunge la factorii de decizie politici. Potrivit unui reprezentant MI6 de la Washington, „un raport DISTANT nu ar trebui considerat de Marea Britanie o certitudine decât în cazul în care JIC hotărăşte acest lucru”. În schimb, opinia CIA, influenţată probabil de experienţa Pearl Harbor, a fost că mesajul ar trebui să parvină imediat factorilor de decizie politici; singura concluzie (deşi critică) rezultată de aici ar recomanda, înainte de toate, confirmarea sursei. Jerold L. Schecter şi Peter S. Deriabin, *The Spy Who Saved the World* (Scribner, New York, 1992), pp. 284 – 286.

13. Eliot A. Cohen, „Analysis”, în Roy Godson (ed.), *Intelligence Requirements for the 1990’s*: *Collection*, *Analysis*, *Counterintelligence and Covert Action* (Heath, Lexington, Lexington, Mass., 1989), p. 83.

14. Kent, „Preface to the 1966 Edition”, *Strategic Intelligence*, p. XXIV.

15. Kent, „Preface”, pp. 58 – 59 [subliniere în original].

16. Într-o anumită măsură, extinderea rolului analitic al serviciilor de informaţii din Statele Unite a fost rezultatul unei anomalii istorice

cauzate de existenţa unui adversar de talia Uniunii Sovietice în perioada postbelică. În timp ce alte ţări consideră că este firesc să dea publicităţii anumite informaţii, ruşii le tratează ca secrete de stat. În consecinţă, toate tipurile de date care altminteri nu ar fi fost decât simplă rutină şi care, din punctul de vedere al tradiţionaliştilor, nu ar fi de competenţa serviciilor secrete au devenit obiectul activităţii de culegere a informaţiilor şi, implicit, de analiză. Deşi într-un mod diferit faţă de teoriile lui Kent referitoare la natura strategică a informaţiilor secrete, lipsa de deschidere a Uniunii Sovietice confirmă, la nivel concret, ideea că serviciile secrete sunt interesate de toate datele care au relevanţă în plan strategic.

17. După cum am mai menţionat, capitolul 6, secţiunea referitoare al „serviciile secrete imperiale”.

18. Concepţia despre importanţa analizei informaţiilor strategice şi motivele care stau la baza acesteia a fost enunţată pentru prima dată de către Kent şi colegii săi în cursul activităţii desfăşurate în cadrul Departamentului de Cercetare şi Analiză a OSS, în timpul celui de-al Doilea Război Mondial. Potrivit istoricului Barry Katz, în faţa ostilităţii acestei birocraţii adânc înrădăcinate şi, în absenţa unei structuri stabile care să monitorizeze această activitate, singura modalitate de protecţie aflată la îndemâna Departamentului [nou-înfiinţat] a fost vălul invizibil al obiectivităţii sociale… în mod surprinzător, ideea unei examinări atente a acestei obiectivităţi, bazată pe «o analiză generală a

procesului de gândire ştiinţifică din sfera socialului», a fost susţinută întotdeauna în timpul războaielor la care a fost martor aceste Departament. [în opinia lui Kent], poziţia «oficială» s-a datorat mai ales acelor domenii de activitate la care cercetătorii americani din cadrul Departamentului de Cercetare şi Analiză se pricepeau cel mai bine, respectiv «acea sferă a ştiinţei cunoscută, în general, ca sociologie». În toate aceste discipline, antinomiile dintre fapt şi valoare, erudiţie şi spiritul partizan cu care Max Weber s-a luptat cu atâta eroism au fost în mare parte estompate… a venit vremea sociologilor, a economiştilor şi informaticienilor… Aşa cum credibilitatea politică a Departamentului depindea de imaginea profesionalismului dezinteresat, credibilitatea epistemologică a disciplinelor se bazează pe o obiectivitate pozitivistă, care poate fi definită în teorie şi doar aproximată în practică". Barry M. Katz, *Foreign Intelligence*: *Research and Analysis in the Office of Strategic Services, 1942 – 1945* (Harvard University Press, Cambridge, Mass., 1989), pp. 14 – 15.

19. În februarie 1992, cele două comisii ale Congresului Statelor Unite pentru serviciile de informaţii au propus norme legislative care să reorganizeze din temelii comunitatea americană a serviciilor de informaţii. Unul dintre principalele proiecte de lege se referea la înfiinţarea unei structuri centralizate de analiză, care să coordoneze toate instituţiile de analiză din cadrul comunităţii de informaţii. În plus, noul centru de analiză, creat după modelul unei structuri

academice, ar fi independent de celelalte componente operative din cadrul comunităţii şi de instituţiile guvernamentale ce reprezintă factori de decizie în stat. Potrivit preşedintelui Comisiei pentru activitatea de informaţii din cadrul Camerei Reprezentanţilor, congresmenul Dave McCurdy, reorganizarea a avut ca principal scop „crearea unui «grup de experţi» de prim rang”. „Intelligence Committee Chairmen Introduce Sweeping Reorganization plan”, Press Release, US Senate Select Committee on Intelligence, 5 februarie 1992. Vezi şi David L. Boren, „The Intelligence Community: How Crucial”, *Foreign Affairs*, 71, nr. 3 (vara 1992), p. 61. Senatorul Boren era, la vremea respectivă, preşedintele Comisiei senatoriale pentru activitatea de informaţii şi susţinătorul propunerii legislative privind reorganizarea serviciilor de informaţii.

20. Vezi, de exemplu, recomandările lui Stansfield Turner incluse în memoriile sale despre activitatea în cadrul serviciilor secrete: *Secrecy and Democracy*: *The CIA* in *Transition* (Houghton Mifflin, Boston, 1985; Harper and Row, New York, 1986). După ce a lansat propunerea privind înfiinţarea unei Agenţii a Porţilor Deschise, care să furnizeze întregii lumi informaţii obţinute prin satelit, acesta a conchis: „Capacităţile noastre din sfera serviciilor de informaţii sunt în deplină concordanţă cu rolul special pe care ni l-am asumat pentru apărarea propriei securităţi şi bunăstarea întregii omeniri, după ce ne-am revizuit propria concepţie despre necesitatea confidenţialităţii informaţiilor în cadrul proceselor

democratice pe care se bazează guvernul nostru… Avem extraordinara şansă de a demonstra superioritatea sistemului nostru democratic, care îşi foloseşte capacităţile din domeniul serviciilor de informaţii nu numai în folosul propriei naţiuni, ci al întregii lumi şi umanităţi" (p. 285).

21. Colby, „Intelligence in the 1980's", p. 69.

22. Pentru o expunere care vine în sprijinul surselor secrete tehnice în această nouă eră, vezi *supra*, capitolul 2, nota 86. Indiferent dacă sursele secrete tehnice sau cele umane vor avea întâietate în obţinerea informaţiilor secrete de importanţă deosebită în plan strategic, fără îndoială că, aşa cum s-a arătat în capitolul 2, sursele secrete tehnice – care încercau altă dată să răspundă cerinţelor factorilor de decizie naţionali – vor avea un rol important în furnizarea informaţiilor secrete de ordin tactic comandanţilor de pe câmpul de luptă.

23. Kent, *Strategic Intelligence*, p. VIII [sublinierea noastră].

24. Pentru la acest aspect şi probleme conexe, vezi Thomas F. Troy, „The «Corect» Definition of Intelligence", *International Journal of Intelligence and Counterintelligence*, 5, nr. 4 (iarna 1991 – 1992), pp. 443 – 454.

25. Turner, *Secrecy and Democracy*, pp. 279 – 285. Turner nu precizează dacă este dispus să pună la dispoziţia întregii omeniri mijloacele tehnice americane de culegere a informaţiilor sau datele obţinute prin astfel de mijloace. Acesta afirmă că, pentru început, „*am putea*" [sublinierea noastră] să furnizăm numai „informaţiile obţinute

cu ajutorul sistemelor perimate, care nu mai reprezintă o noutate" pentru adversar (p. 282). Totodată, consideră că „nu peste mult timp fotografiile obţinute prin satelit vor fi atât de fidele, încât diferenţele dintre diverse tipuri de sateliţi vor fi nesemnificative" (p. 280).

26. Acest citat şi următorul sunt preluate din Colby, „Intelligence in the 1980's", p. 69.

27. Desigur, comiterea unui act de trădare la adresa unui regim tiranic sau agresiv poate fi justificată din punct de vedere moral. Pentru Ryszard Kuklinski, ofiţerul din armata poloneză care a trecut de partea Statelor Unite şi i-a spionat pe ruşii ce îi asupreau ţara natală, motivaţia era de ordin ideologic, astfel că ofiţerii de informaţii din Vest nu au fost nevoiţi să-l manipuleze sau să-l corupă în vreun fel. În alte cazuri însă, când motivaţia o reprezintă banii sau spiritul de aventură, ofiţerul de informaţii trebuie să exploateze punctele slabe ale potenţialului spion pentru a-l determina să cedeze mai repede. Pentru o expunere mai detaliată pe marginea acestui subiect, vezi E. Drexel Godfrey Jr.,"Ethics and Intelligence", *Foreign Affairs*, 56, nr. 3 (aprilie 1978), pp. 624 – 642, şi răspunsul lui Arthur L. Jacobs din „Comments and Correspondence", *Foreign Affairs*, p. 56, nr. 4 (iulie 1978), pp. 867 – 875.

28. Sun Tzu, *The Art of War*, pp. 63 – 64 (capitolul 1, paragrafele 2 – 4).

29. Sun Tzu, *The Art of War*, p. 144 (capitolul 13, paragraful 2).

30. Henry L. Stimson şi McGeorge Bundy, *On*

*Active Service în Peace and War* (Harper, New York, 1948), p. 188. Probabil că Stimson nu a făcut această remarcă la vremea respectivă, ci şi-a exprimat opinia ulterior, în timp ce-şi justifica decizia legată de evenimentele din 1929, când „toată lumea făcea tot posibilul în direcţia menţinerii păcii, iar toate naţiunile erau prietene", precum şi pe cea de a sprijini (în calitate de secretar de stat pe probleme de război) cercetările în domeniul criptanalizei. Este puţin probabil însă ca al Doilea Război Mondial să fi înregistrat atât de multe succese fără eforturile depuse în prealabil în această direcţie. De exemplu, eforturile americanilor de a decoda maşina japoneză de criptat Purple, folosită pentru prima dată în 1939, au fost încununate de succes, depinzând în principal de decodarea maşinii de criptat Red, care data din 1931. Vezi Ronald Lewin, *American Magic*: *Codes*, *Ciphers and the Defeat of Japan* (Farrar Strauss Giroux, New York, 1982), pp. 42 – 43. Pentru o privire de ansamblu asupra serviciilor de informaţii în perioada interbelică, vezi Robert G. Angevine, „Gentleman Do Read Each Other's Mail: American Intelligence in the Interwar Era", *Intelligence and National Security*, 7, nr. 2 (aprilie 1992), pp. 1-29.

31. Vezi, de exemplu, expunerea lui David Kahn pe această temă: „În cartea sa *Perpetual Peace*, Immanuel Kant susţinea că spionajul este o crimă la adresa ordinii mondiale şi că, dacă ar ieşi la iveală, ar crea importante probleme internaţionale. Dar acest lucru nu pare să se întâmple şi în cazul *sigint* (informaţii obţinute din

interceptarea semnalelor şi comunicaţiilor electronice)”. Roy Godson (ed.), *Intelligence Requirements for the 1980’s*: *Clandestine Collection* (Naţional Strategy Information Center, Wasfüngton, DC, 1982), p. 120. În realitate însă, dezvăluirea făcută în 1931 de Herbert Yardley, director al American *Black Chamber* (Camera Neagră), potrivit căreia Statele Unite au interceptat mesajele cifrate dintre Tōkyō şi delegaţia japoneză care a participat la conferinţa Forţelor Navale de la Washington privind limitarea marinei din punct de vedere militar (1921 – 1922), a creat senzaţie în întreaga Japonie. *The American Black Chamber* (Bobbs-Merrill, Indianapolis, 1931; reprint, Ballantine, New York, 1981), pp. 187 – 211. În mod asemănător, E. Drexel Godfrey Jr., fost ofiţer CIA, susţine că „sateliţii de recunoaştere fotografică şi vocală, precum şi alte dispozitive de interceptare sunt extrem de costisitoare, dar prezintă avantajul că aduc atingere numai într-o mică măsură standardelor etice ale angajaţilor şi angajatorilor”. „Ethics and Intelligence”, p. 637.

Capitolul 8. Elemente pentru o teorie a culegerii informaţiilor

1. După cum am precizat în capitolul 1, prezentarea pe trei planuri a serviciilor de informaţii – informaţii, activitate şi structură – este extrasă din Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton University Press, Princeton, NJ, 1949; reprint 1966). Kent însă nu este de părere că restrângerea accesului altor persoane la date reprezintă parte integrantă a activităţii de

informaţii.

2. Kent, *Strategic Intelligence*, pp. 3 – 4.

3. În timpul războiului este necesară folosirea unor mijloace tehnice şi secrete (cum sunt informările agenţilor sau comunicaţiile interceptate) pentru obţinerea unor informaţii privind condiţiile meteorologice de pe teritoriul inamicului. Pentru aceste informaţii am putea folosi denumirea „informaţii meteorologice secrete”. Cu toate acestea, termenul *secrete* se referă la mijloacele prin care sunt obţinute datele neprelucrate, nu la informaţiile meteorologice care permit sau care stau la baza prognozei timpului probabil.

4. Aşa cum scria Willmoore Kendall în 1949 într-o recenzie a cărţii lui Kent: „Cursul evenimentelor este perceput [de starea de spirit reflectată în cartea lui Kent] nu ca un lucru care poate fi influenţat, ci ca o bandă înregistrată aflată într-un aparat; iar sarcina serviciilor de informaţii este să afle ce este pe ea”. „The Function of Intelligence”, *World Politics*, 1, nr. 6 (iulie 1949), p. 549.

5. Kent, *Strategic Intelligence*, p. viii [sublinierea noastră].

6. William E. Colby, „Intelligence for the 1980’s”, *The Information Society*, 1, nr. 1 (1981), p. 59.

7. Pentru această interpretare a relaţiei dintre informaţiile secrete şi cele obţinute din surse deschise, îi rămânem îndatoraţi lui Michael Herman, de la Nuffield Collège, Oxford, care a introdus propunerea pe agenda Convenţiei din

1989 a International Studies Association. De asemenea, informaţiile obţinute din surse deschise pot fi culese de o agenţie secretă înainte ca ele să dobândească un caracter secret. De exemplu, în timpul războiului datele (cum sunt informaţiile referitoare la sistemele de transport sau rezervele de materiale strategice dintr-o anumită ţară) care pe timp de pace sunt accesibile publicului larg capătă caracter de secret de stat, fiind astfel protejate de guvern. În acest caz, culegerea informaţiilor din surse deschise presupune evitarea potenţialelor bariere de securitate ce ar putea bloca accesul la informaţii pe viitor.

8. Avi Shlaim, „Failure în National Intelligence Estimates: The Case of the Yom Kippur War", *World Politics*, 28, nr. 3 (aprilie 1976), p. 355.

9. Analiştii din serviciile de informaţii fac uneori diferenţă între „secrete" şi „mistere". Secretele sunt informaţii existente, la care nu există acces direct. Un exemplu ar fi grosimea blindajului noului tip de tancuri inamice; este evident că inamicul deţine această informaţie, dar face tot posibilul pentru a-i împiedica pe alţii să o afle. În schimb, misterele sunt informaţiile de care nimeni nu este sigur. De exemplu, va folosi oare inamicul noile tancuri pentru a-şi ataca vecinii în următorii zece ani? Chiar dacă inamicul s-a hotărât să atace peste trei ani, nu are de unde să ştie dacă nu se va răzgândi între timp. Kent sugerează că informaţiile strategice cu caracter secret ar putea dezlega misterele sau, cel puţin, ar fi mult mai eficiente decât orice altă metodă.

10. Kent, *Strategic Intelligence*, pp. 206 – 207.

11. În opinia lui Kent, acestea mai sunt cunoscute şi ca date furnizate „pe loc” sau, mai informai, „la minut” (Kent, *Strategic Intelligence*, pp. 28 – 29). Un serviciu de informaţii precum CIA reprezintă un model de referinţă, având atribuţii similare serviciului pentru cercetare din cadrul Bibliotecii Congresului American.

12. William E. Colby, *Honorable Men*: *My Life in the CIA* (Simon and Schuster, New York, 1978), p. 245.

13. Ray S. Cline, *The CIA*: *Reality vs*. *Myth*, ediţie revăzută (Acropolis, Washington, DC, 1982), p. 175.

## Postfaţă

Dintr-o perspectivă americană, *Războiul tăcut* (*Silent Warfare*) reprezintă o trecere în revistă cuprinzătoare a lumii informaţiilor care se adresează simultan neiniţiatului (simplul cetăţean curios), publicului larg, dar şi persoanelor profund implicate – prin natura funcţiei/atribuţiilor lor – în activitatea de informaţii. Beneficiind de ghizi „din interior" (aşa cum o dovedeşte o simplă privire asupra multiplelor însărcinări şi preocupări de studiu ale celor doi autori, Abram N. Shulsky şi Gary J. Schmitt), cartea creează un itinerar logic şi succint prin labirintul plin de mistere al unei lumi mult prea adesea neînţelese şi – în România în mod cert – aproape necunoscute.

Succesiunea capitolelor, care beneficiază de o bibliografie extensivă – suficientă pentru a capta pe termen lung interesul cercetătorilor diferitelor epoci şi episoade din „războiul tăcut", dar şi pentru a stârni imaginaţia organizaţională a decidenţilor politici şi a conducătorilor serviciilor de informaţii dornici să-şi optimizeze performanţele în noul mediu strategic al secolului XXI –, are o rigoare de manual. Din acest ultim punct de vedere, *Războiul tăcut* reprezintă un instrument extrem de util pentru introducerea publicului românesc – atât cel larg, cât şi cel avizat, preocupat de studiile de securitate – în logica teoretică a unui domeniu de activitate care, deşi atractiv, a rămas în mare parte puţin cercetat şi adesea chiar neiubit.

Departe de a-i crea complexe cititorului,

autorii – Abram N. Shulsky şi Gary J. Schmitt – evocă pe scurt, în „Introducere. A scrie despre secrete” (pp. 19 – 22), situaţii din ultimul sfert de secol în SUA ce reprezintă, în esenţă, o încurajare pentru cititorul român să persevereze pe calea cunoaşterii.

De asemenea, însăşi perioada – un sfert de secol – necesară pentru ca întrebările şi dezbaterile despre serviciile de informaţii să nu mai constituie „motiv doar de scandal şi discuţii în contradictoriu”, ci să fie „acceptate ca un aspect normal al dezbaterilor publice privind activităţile guvernamentale în genere” sugerează că demersul editorului român de a ne propune spre lectură *Războiul tăcut* este oportun, dar nicidecum prematur şi cu atât mai puţin suficient.

Elementele tulburătoare ce au adus în actualitatea internaţională problematica informaţiilor şi a structurilor/serviciilor naţionale specializate în culegerea de informaţii au apărut, integral, în anii de după 2001, când lucrarea lui Shulsky şi Schmitt fusese deja revizuită pentru tipar ia a treia ediţie. Este vorba despre emergenţa Al-Qaida pe piaţa globală a ameninţărilor de securitate, prin multiplul atentat din 11 septembrie 2001, despre intervenţia antitalibană din Afganistan, controversele pe marginea programului privind armele de distrugere în masă dezvoltat de Irakul lui Saddam Hussein, dar şi – în desfăşurare încă – evoluţiile din dosarele nucleare nord-coreean şi iranian. Din acest punct de vedere, s-ar putea aprecia că *Războiul tăcut* este doar un mic apetitiv…

În schimb, diferenţele fundamentale de acquis conceptual/teoretic dintre democraţiile vechi, în special cele anglo-saxone, unde încă din anii ’70 a existat o anumită transparenţă în relaţia servicii de informaţii – decidenţi – public (academic sau larg), şi restul statelor, în special tinerele democraţii, unde abordarea problemei informaţiilor de securitate a fost multă vreme interzisă, apoi parţial revendicată de incursiunile istorice pe cazuri de spionaj, defectori sau abuzuri ale structurilor interne de contrainformaţii profilează un potenţial deficit de comunicare între societăţi confruntate în mare măsură cu aceleaşi ameninţări într-o lume globalizată.

Iată aşadar raţiunile pentru care, fără a fi o lucrare ştiinţifică de ultimă oră în domeniul informaţiilor, *Războiul tăcut* vine să arunce o binevenită punte între tradiţia şi trecutul lumii informaţiilor, pe de o parte, şi provocările prezentului, pe de altă parte. O punte pe care lectorul român o va aprecia cu atât mai mult cu cât, prin cazuistica invocată (cazul Enigma – supercifrul german „spart” de britanici în timpul celui de-al Doilea Război Mondial, de exemplu, cunoscut prin traduceri publicate şi în România, în anii ’80) şi prin ancorarea în probleme încă sensibile, cum ar fi controlul democratic asupra serviciilor de informaţii, cartea atrage şi se citeşte cu interes, deşi nu cu sufletul la gură.

Capitolul 1 – „Ce este activitatea de informaţii?” – fixează limitele cunoaşterii comune, implicit punctele de disonanţă asupra cărora mai este de lucrat, la nivel naţional şi internaţional.

Autorii evidenţiază – fără a căuta să ofere însă un răspuns unic sau un evantai de opţiuni – absenţa unei definiţii universale a securităţii, calarea ei tradiţională excesivă pe interesele unui stat anume şi dependenţa de regimul/sistemul de guvernare al acestuia, ca şi centrarea de până acum a sistemelor şi culturii de securitate pe culegerea de informaţii. În legătură cu aceasta din urmă este schiţată principala dilemă a erei informaţiilor – cum îşi păstrează serviciile de informaţii relevanţa în epoci de abundenţă, în care multitudinea informaţiilor determină, pe de o parte, incapacitatea de a le gestiona integral în timp real, iar pe de altă parte, multiplicarea centrelor alternative de analiză/integrare a acestora.

Capitolul 2 – „Spioni, maşini şi biblioteci: culegerea informaţiilor” – constituie o trecere în revistă esenţializată a fundamentelor activităţii serviciilor de informaţii şi implicit o trimitere la principalele elemente spectaculoase ce reprezintă marca distinctivă a spionajului: sursele umane şi mijloacele tehnice de culegere a informaţiilor. Tratate pragmatic, problemele acoperirilor convenţionale şi neconvenţionale sunt ilustrate cu cazuri devenite nu doar istorie, ci uneori film şi literatură (de exemplu, Richard Sorge, Fritz Kolbe, Edward Lee Howard, pp. 39 – 43). Nu lipsesc problemele generate de loialitatea/ fiabilitatea surselor, de „informaţiile prefabricate” ale unor surse interesate, de agenţii dubli, ca şi referirile la arta culegerii datelor sau rapida evocare a „scrierilor secrete” şi a „micropunctelor” sau rolul

defectorilor în culegerea de informaţii, ilustrat prin cazul lui Hussein al-Kamal, ginerele lui Saddam Hussein, care a defectat în 1995, după Războiul din Golf. Referindu-se la sursele tehnice, autorii trec în revistă informaţiile rezultate din fotografii şi imagistică(*imint*), extragerea unor date din unde electromagnetice interceptate (*sigint*) şi alte subspecializări din sfera informaţiilor tehnice (*comint*, *telint*, *masint* etc.) într-un format care poate fi asimilat definiţiei exemplificate a acestora.

În cea mai interesantă parte a capitolului Shulsky şi Schmitt realizează o comparaţie între între sursele umane(*humint*) şi cele tehnice (*techint*), folosindu-se de argumente din dezbaterea publică desfăşurată de-a lungul mai multor decenii în SUA între specialişti. Deosebit de utilă este punctarea interesului serviciilor de informaţii pentru „ţintele dificile” (de tipul societăţilor închise, cum este Coreea de Nord), pentru care *techint* reprezintă soluţia obţinerii informaţiilor. În aprecierea autorilor, sfârşitul Războiului Rece a dus ia diminuarea drastică a necesităţii culegerii tehnice de informaţii şi la o creştere exponenţială a necesităţii de informaţii din surse umane – accentuând importanţa cunoaşterii intenţiilor şi conceptelor strategice ale adversarului/ competitorului, dar şi a obţinerii unor indicii care să orienteze activitatea de interpretare (*sense-making*) a datelor brute obţinute de sistemele şi platformele de culegere a informaţiilor din surse tehnice. Complementaritatea acestor sisteme şi utilitatea

produsului funcţionării lor pentru decizia naţională strategică sunt oportun subliniate de autori. Rămâne însă un mic regret că analiza problemei nu a putut fi aprofundată, pornind de la învăţămintele ultimilor ani, în condiţiile bătăliei difuze pentru securitate naţională şi globală purtate cu forţele teroriste, de exemplu.

Mult mai succintă, secvenţa de text dedicată culegerii de informaţii din surse deschise are chiar un caracter schematic şi incomplet, mai degrabă ancorat în realităţile anilor ’80-*90: presă şi emisiuni radio şi TV, rapoarte diplomatice şi militare sau ale echipelor speciale de inspecţie care furnizează informaţii nu secrete, ci publice, cu circulaţie limitată în medii specializate. Realităţile anului 2008 diferă însă mult prin faptul că mediul virtual – în care se interacţionează adesea spontan şi nestructurat, dar nu neapărat numai aşa, lumea forumurilor şi blogurilor – este în aceeaşi măsură purtător de informaţie şi mult mai dinamic, dar scapă – probabil din raţiuni de claritate a demersului – atenţiei celor doi autori.

Capitolul 3, intitulat sugestiv „Ce înseamnă toate acestea? Analiza şi producerea informaţiilor”, trece în revistă gama de tehnici analitice de „transformare a informaţiilor care sunt culese în orice mod într-un produs care poate fi folosit de factorii de decizie şi liderii militari”. Cu toate ambiţiile de exhaustivitate şi în ciuda intenţiei de a reliefa rolul-cheie al analizei/analistului în formularea concluziilor şi previziunilor care fundamentează decizii majore, cu impact strategic, autorii cedează unui

relativism (analiza nu are categorii standard, în plus categoriile ce există nu sunt nici exacte, nici nu se exclud reciproc – vezi pp. 126 – 127) care transformă presupusa superioritate conferită de raţionament şi gândire critică într-o cauză confuză. Probabil, din dorinţa de a menţine cititorul conectat la lectură, spaţiul cel mai extins este alocat criptanalizei şi altor aspecte tehnice în care cuvintele *cod* şi *cifru* funcţionează ca un fel de „cârlig verbal" pentru a atrage cititorul familiarizat cu thrillerele. Mult mai bine realizată şi cu mai multă relevanţă pentru înţelegerea completă a finalizării muncii de informaţii (spionaj) prin produsul analitic destinat decidentului este partea intitulată „Produsul activităţii serviciilor de informaţii" (pp. 100 – 107), care ilustrează diversitatea de forme pe care le poate îmbrăca informarea pornind de la practicile curente din SUA.

În aceeaşi notă centrată pe analiză, din păcate cu o prejudecată reductivă, sunt tratate eşecurile serviciilor de informaţii. Textul corespunzător abundă în formulări de tipul: „riscul ca serviciile de informaţii să nu evalueze corect o situaţie", „absenţa avertizărilor cu privire la o schimbare economică majoră şi rapidă", „neanticiparea unor evenimente politice sau economice", „o viziune eronată asupra lumii înconjurătoare", „înţelegerea incorectă a unei situaţii, fapt ce determină un guvern... să întreprindă acţiuni inadecvate sau contraproductive din perspectiva intereselor sale", „estimarea incorectă a unui proces sau a unei

situaţii de durată”. Deosebit de tranşantă, dacă privim prin prisma actualelor ameninţări de securitate, pare afirmaţia: „Cu excepţia cazurilor în care nu pot fi obţinute niciun fel de informaţii relevante, eşecurile din activitatea de informaţii sunt legate de o dereglare a procesului analitic, ce determină ignorarea sau interpretarea greşită a datelor” (p. 111). Având în vedere faptul că actualele ameninţări de securitate, în special cele generate în binomul terorism radical – crimă organizată, cunosc evoluţii care în general „se strecoară sub radar”, probabilitatea ca în actuala etapă eşecurile analitice să fie preponderent cauzate de lipsa informaţiilor relevante, lipsa surselor sau a accesului la medii-ţintă dificile şi „exclusiviste” este cel puţin la fel de – dacă nu substanţial mai – ridicată ca şi cea a unei erori de judecată. Cu toate acestea, capitolul continuă cu evidenţierea posibilelor soluţii la eşecuri, reliefând deosebit de corect responsabilităţile managementului serviciilor de informaţii, dar mai ales pe cele ale decidenţilor, care sunt atât beneficiarii finali ai informărilor, cât şi factorii modelatori permanenţi ai activităţii din lumea informaţiilor, de la prioritizarea spaţiilor şi temelor de interes până ia feedbackul corectiv care creşte gradul de adecvare a acţiunii serviciilor de informaţii la nevoile strategice naţionale.

„În culise: operaţiunile secrete”. Sub acest titlu, capitolul 4 ridică parţial vălul misterului care a alimentat, de-a lungul timpului, o bogată literatură sau filmografie, dar şi numeroase

acţiuni de propagandă ori scenarii conspiraţioniste, descriind modul în care se pot promova nemijlocit obiective naţionale de politică externă prin acţiuni ascunse. Într-o gradaţie de la alb la negru sunt descrise pe scurt acţiunile de asistenţă acordată unor state aliate, agenţii de influenţă şi propaganda anonimă, dar şi sprijinul pentru loviturile de stat, „războaiele de eliberare naţională" şi „luptătorii pentru libertate". Din gama operaţiunilor are au suscitat cele mai aprige controverse – în SUA, dar şi în mediul internaţional – în diferite etape istorice autorii nu exclud nici câtva exemple de *wet affairs* (eufemism pentru asasinat şi sabotaj), cum ar fi cazul aruncării în aer de către agenţi francezi, în 1985, a vasului *Rainbow Warrior* aparţinând organizaţiei ecologiste Greenpeace. Pentru cititorul tânăr, sub 30 de ani, trecerea în revistă, deşi succintă, a unor cazuri celebre din anii '60—80, în explicitarea rolului şi limitelor confidenţialităţii în operaţiunile secrete, se poate dovedi extrem de instructivă, cu atât mai mult cu cât este susţinută de o bogată bibliografie care, accesată, poate satisface curiozităţi tehnice, dar mai ales istorice mai profunde. Prin aceasta, capitolul – care în esenţă rezonează cu preocupări foarte specifice din SUA, legate, de exemplu, de plasarea operaţiunilor secrete în organigrama unui anumit serviciu de informaţii sau transparenţa dezbaterilor în Congres cu privire la acestea – se salvează şi găseşte o utilitate şi pentru cititorul internaţional, neconfruntat în ţara sa cu astfel de probleme.

„Spion contra spion: activitatea de contrainformaţii” reprezintă substanţa capitolului 5. Păşind în „groapa cu lei”, spaţiul de înfruntare dintre servicii de informaţii concurente/adversare, Shulsky şi Schmitt explicitează importanţa prevenirii accesului neautorizat la informaţiile de importanţă pentru stat. Absolut firesc, măsurile pasive enunţate includ clasificarea informaţiilor care trebuie protejate, exemplificând efectele dezvăluirii acestora unor persoane neautorizate, ca şi principiul „nevoii de a cunoaşte”, fără a eluda însă capcanele supraclasificării. Interesante sunt paginile dedicate subclasificării informaţiilor, care, rară a se concretiza în propunerea unei definiţii cuprinzătoare a securităţii naţionale, o prefigurează, evocând categoriile de informaţii generate în afara sferei guvernamentale (în mediul privat, bursier, financiar) care nu sunt supuse sistemului de clasificare, deşi cunoaşterea lor de către persoane sau entităţi neetice poate conduce la daune certe la adresa securităţii naţionale, internaţionale sau a cetăţeanului. Exemplele se referă la sfera tehnologică, informaţii financiare, informaţii personale…

O altă garanţie pe care activitatea de contrainformaţii le-o oferă beneficiarilor de securitate este aceea a integrităţii personalului angajat în serviciile de informaţii. Descrierea autorilor cu privire la securitatea personalului este destul de extinsă, nelipsind nici referirile la celebrul test cu „detectorul de minciuni” (poligraful). Nu lipsesc din prezentare elementele privind securitatea fizică, depăşite însă în

spectaculozitate de măsurile active pe linie de contraspionaj, de la supraveghere şi culegere de informaţii la utilizarea agenţilor dubli şi, ca un corolar, activităţile contrainformative multidisciplinare (MDCI), ce abordează tot spectrul de resurse de care poate dispune un guvern/serviciu adversar.

Un spaţiu destul de extins în economia acestui capitol (pp. 184 – 197) este rezervat dezinformării şi contradezinformării, centrate pe anularea capacităţii de a analiza corect informaţiile secrete, respectiv păstrarea avantajului secretului asupra unor locaţii, capacităţi, intenţii de acţiune. Dezinformarea, ca un virus care alterează rezultatul final al unui întreg ciclu de informare, de la culegerea de date până la prezentarea produsului analitic final unui decident, este „parcursă" etapă cu etapă. Singurul element de frustrare, în această extrem de convingătoare demonstraţie, este vechimea exemplelor utilizate (extrase din istoria bătăliei secrete dintre serviciile de informaţii aliate şi cele germane, în al Doilea Război Mondial, sau din perioada de început a Războiului Rece, anii 1953 – 1961). Înţelegând foarte exact de ce autorii se menţin în limitele informaţiei deja declasificate, cititorul nu se poate abţine totuşi să nu regrete că nu i se oferă măcar exemple ipotetice mai apropiate de realităţile umane şi tehnologice, respectiv de mizele „bătăliei informaţiilor" în însăşi era informaţională.

Destinat în mod explicit altui public decât cele precedente, capitolul 6 abordează, sub un

titlu elocvent („Controlul paznicilor: managementul culegerii informaţiilor”), relaţia dintre „stăpânii politici” (autorităţile cărora li se subordonează serviciile de informaţii) şi managementul acestora. Evidenţiind rapid plusul de integritate şi responsabilitate ce caracterizează normal serviciile de informaţii prin comparaţie cu alte agenţii guvernamentale, Shulsky şi Schmitt schiţează totuşi diferenţa dintre accesul la informaţii şi cunoştinţele suficiente pentru a controla eficient lumea informaţiilor. Spre disperarea scepticilor, ilustrarea oferită acestei situaţii dilematice este însă fundamental favorabilă serviciilor de informaţii, care, prin „negarea plauzibilă” (p. 201), le creează „stăpânilor politici” avantajul de a nu fi niciodată vinovaţi în caz de eşec. (Situaţia este ilustrată cu referire la documentele – sau, mai precis, absenţa acestora – care ar fi dovedit că CIA a primit la începutul anilor ’60 misiunea de a-l asasina pe Fidel Castro.)

Este ilustrată, de asemenea, evoluţia relaţiei serviciu de informaţii – decident, de la cea unipersonală, tipică începuturilor statelor moderne, la o relaţie constituţională, în care executivul şi aleşii, parlamentul, îşi exercită pe deplin atribuţiile prin accesul oficial la informaţii, notificări privind anumite tipuri de activităţi şi cerinţa ca fondurile pentru activităţile informative să fie alocate prin lege.

Deosebit de interesantă este analiza relaţiei expertiză-strategie, respectiv servicii de informaţii – decident politic. Nu scapă ochiului atent al

autorilor situaţiile cele mai frecvente de disonanţă între cele două elemente ale binomului. Dificultăţile relaţiei sunt atribuite de ofiţerii de informaţii tendinţei factorului politic de a ignora informările care nu-i susţin strategiile politice (sindromul „uciderii mesagerului”), situaţie la care singurul răspuns este, după Shulsky şi Schmitt, independenţa agenţiilor de informaţii, care să se ghideze exclusiv după informaţia deţinută, şi nu după modalitatea în care produsul lor analitic ar afecta procesul politic. La celălalt pol, sugestiv identificat prin sintagma „informaţiile imperiale”, accesul direct al decidentului, în special al demnitarului de vârf, la informaţii pe care analistul nu le cunoaşte, cum ar fi conversaţiile confidenţiale cu demnitari străini, face ca factorul politic să considere îndreptăţit refuzul de a renunţa la propriile concluzii în favoarea celor ale unui analist de informaţii anonim. Fără a ascunde influenţa covârşitoare pe care experienţele personale m şi cu ambele „lumi” în discuţie o au asupra propriilor concluzii, autorii evocă – deşi în treacăt – experienţa mai puţin tensionată şi mai cooperantă din Marea Britanie, unde existenţa îndelungată a unor formate de interacţiune permanentă între decidenţi şi serviciile de informaţii1 face din evaluările de securitate o combinaţie de informaţii secrete şi strategie politică.

Pledoaria principală este însă în favoarea independenţei serviciilor secrete, printre ale căror funcţii importante autorii menţionează evidenţierea domeniilor în care strategia politică

nu dă rezultate sau a devenit inadecvată (p. 214). Un alt exemplu de independenţă – a lua iniţiativa de a cerceta probleme sau zone ale lumii fără să fie nevoie de un ordin expres al comunităţii factorilor politici, pentru a depista potenţiale probleme din zonele care nu atrag atenţia celor menţionaţi – pare însă cel puţin în contradicţie deopotrivă cu misiunea de avangardă şi avertizare a serviciilor de informaţii (în fond, raţiunea lor de a exista este de a şti cu un ceas mai devreme, de a evita surpriza strategică) şi cu scepticismul subtextual al autorilor faţă de permanenta conlucrare decident – agenţie de informaţii în stabilirea priorităţilor strategice. Şi aceasta pentru că, în logica controlului, alocarea unor fonduri pentru funcţia de avertizare strategică reprezintă un mandat implicit de scanare a orizontului spre a evita surpriza strategică…

Incluse în acelaşi capitol 6, problemele serviciilor de informaţii în era informaţională sunt tratate extrem de sumar, în puţin peste două pagini, într-o manieră care nu relevă decât partea tradiţionalistă a abordării autorilor, fără a analiza chestiuni fundamentale în momentul de faţă, cum ar fi emergenţa principiului nevoii de a împărtăşi informaţiile (*need to share*, complementar, şi nu contrapus faţă de *need to know*), formele de networking intraservicii, intraguvernamental sau între autorităţii naţionale (politice, de informaţii) şi alte segmente ale societăţii (private, academice). În prelungirea acestor limitări, apare relativ încifrată unui nespecialist – mai ales neamerican – secvenţa tematică dedicată

controlului legislativ şi al societăţii civile asupra serviciilor de informaţii, chiar dacă exemplificările includ şi o paralelă SUA-Canada. În finalul capitolului, o parte relativ lungă (pp. 220 – 240) este dedicata democraţiei, activităţii de contrainformaţii şi de informaţii interne – problemă spinoasă ce combină chestiunea demarcaţiei între acţiunile legitime de culegere a informaţiilor şi cele lipsite de legitimitate cu aspecte legate de infracţionalitate, securitatea personalului – toate iniţial legate de intruziunile în viaţa privată care pot surveni în investigarea pe plan intern a cazurilor de sabotaj, subversiune sau spionaj efectuat de propriii cetăţeni, dar extinse ulterior asupra domeniului emergent al terorismului, inclusiv cel „de casă”(*homegrown*). În aceste secţiuni cartea lui Abram N. Schulsky şi Gary J. Schmitt datează, prin faptul că se bazează atât pe legislaţia anterioară anului 2000, cât şi pe o cazuistică neconvingătoare (atentatul cu bombă asupra sediului FBI din Oklahoma City, din 1995, de exemplu), dacă privim prin prisma dezvoltărilor pe „frontul terorist” punctate, între 2001 şi 2008, cu episoadele sângeroase de la World Trade Center, din Bali, Istanbul, Madrid, Londra, dar şi prin prisma construcţiei legislative şi instituţionale din SUA după 2001 (adoptarea Homeland Security Strategy şi crearea Departamentului de Securitate Internă – Homeland Security Departament –, respectiv adoptarea legislaţiei care a consolidat coordonarea comunităţii informative prin crearea Oficiului Directorului Naţional de Informaţii).

Cu un simţ al gradării tensiunii destul de apropiat de cel al unui romancier, autorii ridică însă cota de interes şi suspans a cărţii în ultimele capitole.

„Două perspective asupra lumii informaţiilor" (capitolul 7) contrapune viziunea „tradiţională" asupra lumii informaţiilor, în care sinonimul perfect al activităţii acesteia este „spionajul", tratat în general pe coordonatele milenare ale *Artei Războiului* a lui Sun Tzu, şi care se bazează pe cunoaşterea secretelor altor puteri în scopul câştigării bătăliei (competiţiei) Şcolii americane avându-l ca prim pilon pe Sherman Kent, fost ofiţer al OSS2 devenit primul şef al Biroului pentru Estimări Naţionale al CIA. În lucrarea sa *Strategice Intelligence for American World Policy*, Sherman Kent – al cărui nume a devenit, în lumea analiştilor de informaţii, aproape un sinonim al analizei ca profesie şi disciplină de studiu – pleda pentru cercetarea bazată pe o metodă sistematică, extrasă din arsenalul ştiinţelor sociale, aplicată simultan ansamblului datelor deţinute – fie ele secrete, fie din surse deschise sau obţinute prin observare directă. În această viziune, fără a minimaliza rolul ofiţerului care culege informaţii, piesa centrală în arhitectura serviciilor de informaţii este analiza, prin *capacitatea sa de a anticipa* evenimente probabile. Ulterior, pe acest fundament, noua viziune americană – din ce în ce mai larg împărtăşită şi în cercuri internaţionale de specialitate – şi-a îmbogăţit metodele şi tehnicile, făcând din analiza informaţiilor – după cum apreciază Shulsky şi Schmitt – o ştiinţă socială

universală şi anticipativă (p. 245). Pe acest teren, în ultimul deceniu discuţiile experţilor în informaţii gravitează tot mai accentuat în jurul problemelor cunoaşterii, ca etapă superioară a culegerii datelor, analizei informaţiilor şi redactării evaluărilor, în acest sens, analiza informaţiilor accede la palierul gândirii strategice, devine parte integrantă a adoptării/aplicării politicilor internaţionale, păstrându-şi însă independenţa faţă de politic cu acribia unui grup de reflecţie performant.

Fără a-i fi deosebit de clar cititorului – în special celui român, care nu deţine fondul de informaţii, percepţii şi situaţii capabil să-i faciliteze decodarea scurtelor, dar denselor paragrafe –, capitolul final, „Elemente pentru o teorie a culegerii informaţiilor”, ratează cu puţin propunerea unei formule teoretice coerente. Cu toate acestea, două sunt meritele sale fundamentale: acela de a da drept de existenţă surselor deschise în „cetatea secretelor”, luând în considerare faptul că obiectivul final este cunoaşterea – mai complexă şi mai utilă decât un secret profund rupt de context –, şi, în final, de a întări sensul activităţilor de informaţii într-o memorabilă frază finală ce reinstituie primatul acţiunii: „Adevărul nu reprezintă un obiectiv, ci un instrument în obţinerea victoriei”.

O victorie pe care, în numele intereselor sale strategice, orice naţiune şi-o doreşte repetată zilnic, an de an, pe o spirală ascendentă a devenirii ei în securitate şi stabilitate.

*

Cartea *Războiul tăcut* a lui Abram N. Shulsky şi Gary J. Schmitt împrăştie aura de mister ce planează asupra lumii informaţiilor, oferindu-i deschidere către înţelegerea raţională a unui domeniu complex, de maximă rigoare şi disciplină, precum şi perspectiva unor aşteptări mai realiste. Toate însă fără a scăpa din vedere caracterul „de echipă" al acestei lumi şi necesitatea coordonării, în activitate, atât cu beneficiarii informaţiilor (decidenţii politici), cât şi cu beneficiarii climatului de securitate ce poate şi trebuie să fie realizat prin activitatea serviciilor de informaţii, respectiv publicul larg sau, individual, cetăţeanul.

Dincolo de această lectură critică, adnotată, rămân o multitudine de aspecte pe care acest reuşit „îndreptar pentru studiu asupra lumii informaţiilor" nu avea spaţiul să le abordeze.

Relaţia decident – serviciu de informaţii înseamnă, de exemplu, o discuţie despre prioritizare, nu numai pentru că evoluăm într-un spaţiu în care cantitatea de informaţie disponibilă în mod deschis creşte zilnic exponenţial, ci şi, poate mai prozaic, pentru că evoluăm într-un spaţiu guvernamental în care resursele sunt transparent alocate, dar niciodată în progresie geometrică. Elemente de detaliu, cum ar fi relevanţa activităţii de informaţii în echilibrul dintre nevoia de informaţie strategică şi cererile punctuale de informaţii ce pot surveni cotidian, coordonarea interinstituţională şi viziunea pe termen lung, atât de necesară laborioasei construiri a unui dispozitiv informativ, şi, în final, dar nu în ultimul rând, relaţia analistului cu

complexitatea mediului contemporan de securitate, multidisciplinaritatea şi managementul cunoaşterii, rămân tot atâtea provocări pe care, putem să sperăm, editorii le vor ilustra, în continuare, prin cărţi de referinţă asemenea volumului de faţă.

*Mihai-Răzvan Ungureanu*